ADVANCES IN MATHEMATICS 32, 83–117 (1979)

On the Multiplicative Complexity of the Discrete Fourier Transform

S. WINOGRAD

IBM Thomas J. Watson Research Center, Yorktown Heights, New York 10598

Most results in multiplicative complexity assume that the functions to be computed are in the field of constants extended by indeterminates, that is, the variables satisfy no algebraic relation. In this paper we extend some of the known results to the case that some of the variables do satisfy some algebraic relations. We then apply these results to obtaining a lower bound on the multiplicative complexity of the Discrete Fourier Transform. In the special case of computing the Discrete Fourier Transform of a prime number of points, the lower bound is actually attainable.

I. INTRODUCTION

Let G be a field, $\{x_0, x_1, \ldots, x_{n-1}\}$ and $\{y_0, y_1, \ldots, y_{n-1}\}$ two sets of indeterminates, and let $P(u)$ be a monic polynomial of degree n with coefficients in G. Denote by $R(u)$ the polynomial $R(u) = \sum_{i=0}^{n-1} x_i u^i$ by $S(u)$ the polynomial $S(u) = \sum_{i=0}^{n-1} y_i u^i$ and by $C(P)$ the set of coefficients of the polynomial $T(u) = R(u) \cdot S(u) \mod P(u)$. The multiplicative complexity of $C(P)$ was studied in [1] and [2]. It was shown that if P is irreducible, or even a power of an irreducible polynomial, the minimum number of multiplications needed to compute $C(P)$ is $2n - 1$. The more general case of simultaneously computing the set $C(P_1) \cup C(P_2) \cup \cdots \cup C(P_l)$ was also considered in [1]. If each of the polynomials P_i is a power of an irreducible polynomial, and the coefficients of all the R_i's and S_i's are distinct indeterminates, then the minimum number of multiplications needed to compute $C(P_1) \cup C(P_2) \cup \cdots \cup C(P_l)$ is $\sum_{i=1}^{l} (2 \deg(P_i) - 1)$. Moreover, every algorithm which uses the minimum number of multiplications necessarily computes each $C(P_i)$ separately. In case P is not a power of an irreducible polynomial, then P can be written as $P = \prod_{i=1}^{l} P_i$ where each P_i is a power of an irreducible polynomial, and $(P_i, P_j) = 1$ for $i \neq j$. As a consequence of the Chinese Remainder Theorem, computing $C(P)$ is equivalent to computing $C(P_1 \cup C(P_2) \cup \cdots \cup C(P_l)$, and therefore the minimum number of multiplications needed to compute $C(P)$ is $2 \deg P - l$.

These results were used in [3] to obtain a new algorithm for computing the Discrete Fourier Transform. One of the steps in obtaining the new algorithm

0001-8708/79/050083-35$05.00/0

Copyright © 1979 by Academic Press, Inc.
All rights of reproduction in any form reserved.

dealt with the computation of the Discrete Fourier Transform of p points, where p is a prime number. In this case computing the Discrete Fourier Transform is tantamount to computing the cyclic convolution of two $(p-1)$ dimensional vectors. The first vector has as entries some powers of w ($w = e^{2\pi i/p}$) and the second, the set of points to be transformed. Since computing the cyclic convolution of two n dimensional vectors (with indeterminates entries) is the same as computing $C(u^n - 1)$, the results of [1] were used to obtain the new algorithm.

However, the proof of the minimality of the number of multiplications given in [1] assumed that the coefficients of $R(u)$ and $S(u)$ are indeterminates, i.e., they satisfy no algebraic relation. When we compute the Discrete Fourier Transform of a prime number of points, the coefficients of $R(u)$ are powers of the pth root of unity, and therefore satisfy algebraic relations. The reader's attention is called to the FFT [4] where algebraic relations are heavily used to derive the algorithm. (It should be pointed out that FFT does not deal with the Discrete Fourier Transform of a prime number of points.)

The purpose of this paper is to extend the results of [1] to the case where the coefficients of $R(u)$ may satisfy algebraic relations. The main result of the paper is a derivation of a lower bound on the number of multiplications needed to compute $C(P_1) \cup C(P_2) \cup \cdots \cup C(P_l)$, where each P_i is an irreducible polynomial, and the coefficients of the $R_i(u)$ may satisfy algebraic relations. In the next section we will give the definitions and some preliminary results, in the following section we will prove the main result, and in Section IV, we will apply the results to the problem of computing the Discrete Fourier Transform.

II. Preliminary Results

To indicate the scope of the results we will start with the definition of the computational process under consideration. The definition given here was first given in [5].

Let G be a field of constants (in most applications, G is the field Q of rational numbers). Let $F \supseteq G$ be a field which includes G, and let $\{y_1, y_2, \ldots, y_n\}$ be a set of indeterminates. Denote by H the field $H = F(y_1, y_2, \ldots, y_n)$. The objects to be computed are $\psi_1, \psi_2, \ldots, \psi_t$ where $\psi_i \in H$ $(i = 1, 2, \ldots, t)$. To start the computation, we assume we are given a set $B \subseteq H$ called a base. We demand, of course, that the ψ's will be elements of the field generated by B. (We will usually assume that $B = F \cup \{y_1, y_2, \ldots, y_n\}$.) The algorithm starts from the elements of B and computes new elements of H by using the field operations. More precisely:

Definition 1. An algorithm $\mathcal{A}$ over a base set B is a finite sequence of

elements (steps of the agorithm) $h_1, h_2, \ldots, h_s$ such that each h_j is either an element of B or $h_j = h_k \circ h_l$ where $k, l < j$ and $\circ$ is one of the field operations. The algorithm is said to compute $\psi_1, \psi_2, \ldots, \psi_t$ if for each i $(i = 1, 2, \ldots, t)$ there exists a j $(1 \leqslant j \leqslant s)$ such that $\psi_i = h_j$.

Intuitively speaking, each step in the algorithm either "calls on" an element of the base set or else performs a field operation on previously computed entities.

In this paper we will consider the number of multiplications/divisions, denoted m/d, which are necessary to perform the computation. The following two definitions make this notion precise.

DEFINITION 2. Let $\mathscr{A}$ be an algorithm over a base set B. A step $h_j \in \mathscr{A}$ is an *essential multiplication/division step* (*an m/d step*) if none of the following holds:

(1) $h_j \in B$

(2) $h_j = h_k \pm h_l$ for some $k, l < j$

(3) $h_j = h_k \cdot h_l$ for some $k, l < j$ such that either $h_k \in G$ or $h_l \in G$

(4) $h_j = h_k : h_l$ for some $k, l < j$ such that $h_l \in G$.

That is, an m/d step of the algorithm $\mathscr{A}$ is a step that could only have been obtained by multiplying two previous steps none of which is in G or by dividing two previous steps where the divisor is not in G.

DEFINITION 3. Let $\mathscr{A}$ be an algorithm over B. We denote by $\mu(\mathscr{A})$ the number of m/d steps in $\mathscr{A}$. For a set of elements $\psi_1, \psi_2, \ldots, \psi_t \in H$, we define the *multiplicative complexity* of $\psi_1, \psi_2, \ldots, \psi_t$ (over B) denoted by $\mu_B(\psi_1, \psi_2, \ldots, \psi_t)$, as $\mu_B(\psi_1, \psi_2, \ldots, \psi_t) = \min_{\mathscr{A}} \mu(\mathscr{A})$, where $\mathscr{A}$ ranges over all algorithms over B which compute $\psi_1, \psi_2, \ldots, \psi_t$. In the case where $B = F \cup \{y_1, \ldots, y_n\}$ we will drop the reference to B and denote the multiplicative complexity of $\psi_1, \psi_2, \ldots, \psi_t$ by $\mu(\psi_1, \psi_2, \ldots, \psi_t)$.

Remark 1. An element $\psi \in H$ satisfies $\mu_B(\psi) = 0$ if and only if $\psi \in L_G(B)$, the linear span (over G) of the base set B. If $\{\psi_1, \psi_2, \ldots, \psi_t\}$ and $\{\phi_1, \phi_2, \ldots, \phi_t\}$ satisfy $\phi_i - \psi_i \in L_G(B)$, $(i = 1, 2, \ldots, t)$, then $\mu_B(\psi_1, \psi_2, \ldots, \psi_t) = \mu_B(\phi_1, \phi_2, \ldots, \phi_t)$; that is, they have the same multiplicative complexity.

In view of Remark 1 we want to identify two elements of H if their difference lies in $L_G(B)$. If we view H as a vector space over G, it is natural to consider the quantities ψ_i to be computed as (representative of) elements in the quotient space $V = H/L_G(B)$. We will use r to denote the natural homomorphism $r: H \to V$.

Remark 2. Let $\mathscr{A}$ be an algorithm over a base set B and J the set of indices j such that h_j is an m/d step. Let $J(i)$ denote the set $J \cap \{1, 2, \ldots, i\}$. For each step i of the algorithm, h_i belongs to $L_G(B \cup \bigcup_{j \in J(i)} h_j)$ the linear space (over G)

of B and all the m/d steps not subsequent to h_i. Put differently, $r(h_i) \in L_G(\bigcup_{j \in J(i)} r(h_j))$. In particular, if $\mathscr{A}$ computes $\psi_1, \psi_2, \ldots, \psi_t$ then for each $i = 1, 2, \ldots, t$, $r(\psi_i) \in L_G(\bigcup_{j \in J} r(h_j))$.

The idea of the proof of the first lemma is due to L. Auslander.

LEMMA 1. *Let $\psi_1 \notin L_G(B)$ (i.e., $r(\psi_1) \neq 0$). For every algorithm $\mathscr{A}$ over B which computes $\{\psi_1, \ldots, \psi_t\}$ there exists an algorithm $\mathscr{A}'$ over $B' = B \cup \{\psi_1\}$ computing $\{\psi_1, \ldots, \psi_t\}$ such that $\mu(\mathscr{A}') \leqslant \mu(\mathscr{A}) - 1$. Moreover, $\mu_B, (\psi_1, \ldots, \psi_t) \leqslant \mu_B(\psi_1, \ldots, \psi_t) - 1$.*

Proof. Since $\mathscr{A}$ computes $\{\psi_1, \ldots, \psi_t\}$, by Remark 2, $r(\psi_1) \in L_G(\bigcup_{j \in J} r(h_j))$. Let s be the smallest integer such that $r(\psi_1) \in L_G(\bigcup_{j \in J(s)} r(h_j))$. Since $r(\psi_1) \neq 0$ then $s \geqslant 1$. Using the minimality of s we obtain that h_s is an m/d step and that $r(h_s) \in L_G(r(\psi_1) \cup \bigcup_{j \in J(s-1)} r(h_j))$. That is, h_s can be expressed as a linear combination (with coefficients in G) of some elements of B, ψ_1, and the m/d steps preceding h_s. Viewing $\mathscr{A}$ as an algorithm over B' we modify it to an algorithm $\mathscr{A}'$ over B' by replacing h_s by a sequence of non m/d steps which compute h_s as this linear combination. By construction $\mathscr{A}'$ has at least one m/d step fewer than $\mathscr{A}$. To prove the second half of the lemma we choose $\mathscr{A}$ such that $\mu(\mathscr{A}) = \mu_B(\psi_1, \ldots, \psi_t)$.

Repeated applications of Lemma 1 yields:

COROLLARY 1. *Let $r(\psi_1), \ldots, r(\psi_k)$ be linearly independent. For every algorithm $\mathscr{A}$ over B computing $\{\psi_1, \ldots, \psi_t\}$ there exists an algorithm $\mathscr{A}'$ over $B' = B \cup \{\psi_1, \ldots, \psi_k\}$ computing $\{\psi_1, \ldots, \psi_t\}$ such that $\mu(\mathscr{A}') \leqslant \mu(\mathscr{A}) - k$. Moreover,*

$$\mu_{B'}(\psi_1, \ldots, \psi_t) \leqslant \mu_B(\psi_1, \ldots, \psi_t) - k.$$

If $\{r(\psi_1), \ldots, r(\psi_k)\}$ are linearly dependent, we can choose a linearly independent subset and express the rest as linear combinations (with coefficients in G) of the linearly independent ones. We thus obtain

COROLLARY 2. *For every algorithm $\mathscr{A}$ over B computing $\{\psi_1, \ldots, \psi_t\}$ there exists an algorithm $\mathscr{A}'$ over $B' = B \cup \{\psi_1, \ldots, \psi_k\}$ computing $\{\psi_1, \ldots, \psi_t\}$, such that $\mu(\mathscr{A}') \leqslant \mu(\mathscr{A}) - d(k)$ where $d(k)$ is the dimension of $L_G(r(\psi_1), \ldots, r(\psi_k))$. Moreover, $\mu_{B'}(\psi_1, \ldots, \psi_t) \leqslant \mu_B(\psi_1, \ldots, \psi_t) - d(k)$.*

In particular, if we take $k = t$ then $\{\psi_1, \ldots, \psi_t\} \subseteq B'$, and therefore by Remark 1, $\mu_{B'}(\psi_1, \ldots, \psi_t) = 0$. We thus obtain a corollary, first proved in [6] *for the case $B = F \cup \{y_1, y_2, \ldots, y_n\}$:*

COROLLARY 3. *Let d be the dimension of $L_G(r(\psi_1), r(\psi_2), \ldots, r(\psi_t))$ then*

$$\mu_B(\psi_1, \ldots, \psi_t) \geqslant d.$$

In the proof of Lemma 1 *we "simulated" the m/d step h_s by a sequence of non m/d steps when we enlarged B to B', and thus obtained a relation between the multiplicative complexity of $\{\psi_1, ..., \psi_t\}$ over the two base sets B and B'. The next lemma yields another relation between the multiplicative complexity of two base sets. Before stating the lemma we need to define a concatenation of two algorithms.*

DEFINITION 4. Let $\mathscr{A} = (h_1, h_2, ..., h_u)$ and $\mathscr{A}' = (k_1, k_2, ..., k_v)$ be two algorithms over B. The algorithm $(\mathscr{A}, \mathscr{A}')$ called the *concatenat on of* $\mathscr{A}$ *and* $\mathscr{A}'$ is the algorithm $(\mathscr{A}, \mathscr{A}') = (h_1, h_2, ..., h_u, k_1, k_2, ..., k_v)^\dagger$, where the dagger indicates that we delete any k_i which is equal to some h_j.

LEMMA 2. *Let C be a finite subset of B, $B' = B - C$, and let C be in the field generated by B'. For every algorithm $\mathscr{A}$ over B which computes $\{\psi_1, ..., \psi_t\}$ there exists an algorithm $\mathscr{A}'$ over B' which computes $\{\psi_1, ..., \psi_t\}$ and such that:*

(1) $\mathscr{A}' = (\mathscr{A}'', \mathscr{A})$ *where $\mathscr{A}''$ is an algorithm over B' which computes C.*

(2) $\mu(\mathscr{A}') = \mu(\mathscr{A}'') + \mu(\mathscr{A})$.

Hence, $\mu_B(\psi_1, ..., \psi_t) \leqslant \mu_B(C) + \mu_B(\psi_1, ..., \psi_t)$.

Proof. Since $\mathscr{A}''$ is an algorithm over B' it is a-forteiori an algorithm of B. So $\mathscr{A}' = (\mathscr{A}'', \mathscr{A})$ (as an algorithm over B) computes $\{\psi_1, ..., \psi_t\}$. But if any step of $\mathscr{A}$ was in C it was deleted in the formation of $(\mathscr{A}'', \mathscr{A})$ by the dagger operation. Thus $\mathscr{A}'$ is also an algorithm over B'. The second condition on $\mathscr{A}'$ follows from the observation that every *m/d* step of $\mathscr{A}'$ is either an *m/d* step of $\mathscr{A}''$ or of $\mathscr{A}$. The second part of the lemma follows by choosing $\mathscr{A}$ such that $\mu(\mathscr{A}'') = \mu_B(C)$.

Combining Lemma 2 and Corollaries 1 and 3 we obtain:

LEMMA 3. *Let $r(\psi_1), r(\psi_2), ..., r(\psi_k)$ be linearly independent, and such that each ψ_i $(i = 1, 2, ..., k)$ satisfies $\mu_B(\psi_i) = 1$ then for every algorithm $\mathscr{A}'$ computing $\{\psi_1, ..., \psi_t\}$ with the property that $\mu(\mathscr{A}') = \mu_B(\psi_1, ..., \psi_t\}$ there exists an algorithm $\mathscr{A}$ over B such that:*

(1) *The first k m/d steps of $\mathscr{A}$ compute $\psi_1, \psi_2, ..., \psi_k$.*

(2) $\mu(\mathscr{A}') = \mu_B(\psi_1, ..., \psi_t)$.

Proof. We now wish to apply Lemma 1. Just to keep the notation confusing, we take B in Lemma 2 as $B' = B \cup \{\psi_1, ..., \psi_k\}$, C in Lemma 2 as $\{\psi_1, \psi_2, ..., \psi_k\}$ and B' of Lemma 2 as B. Lemma 2 then implies that for every algorithm $\mathscr{A}'$ (over B) computing $\{\psi_1, ..., \psi_k\}$ and for every algorithm $\mathscr{A}''$ over $B' = B \cup \{\psi_1, \psi_2, ..., \psi_k\}$ computing $\{\psi_1, \psi_2, ..., \psi_t\}$ that the algorithm $\mathscr{A} = (\mathscr{A}', \mathscr{A}'')$ satisfies the first part of the lemma. In particular, if we choose $\mathscr{A}'$ such that $\mu(\mathscr{A}') = \mu_B(\psi_1, ..., \psi_k)$ and $\mathscr{A}''$ such that $\mu(\mathscr{A}'') = \mu_{B'}(\psi_1, \psi_2, ..., \psi_t)$ then $\mu(\mathscr{A}) \leqslant \mu_B(\psi_1, ..., \psi_k) + \mu_{B'}(\psi_1, ..., \psi_t) \leqslant \mu_B(\psi_1, ..., \psi_k) + \mu_B(\psi_1, ..., \psi_t) - k$ (the

last inequality follows from Corollary 1). By Corollary 3 $\mu_B(\psi_1, \psi_2, ..., \psi_k) \geqslant k$, and by the assumption that $\mu_B(\psi_i) = 1$ $(i = 1, 2, ..., k)$ we have that $\mu_B(\psi_1, ..., \psi_k) \leqslant k$, and therefore $\mu_B(\psi_1, ..., \psi_k) = k$. We thus obtain that $\mu(\mathscr{A}) \leqslant \mu_B(\psi_1, ..., \psi_k)$. But $\mathscr{A}$ is an algorithm over B which computes $\psi_1, ..., \psi_t$ and therefore the inequality must be an equality. This proves that $\mathscr{A}$ satisfies condition 2 as well.

This lemma was first proved in [7] in the special case that $F = G(x_1, ..., x_m)$ (the x_j's are indeterminates), and each ψ_i is a bilinear form of the x_j's and y_j's.

The results derived so far are for an arbitrary base set B. The results which follow are proved in the special case that $B = F \cup \{y_1, ..., y_n\}$. *For the rest of the paper we will assume that* $B = F \cup \{y_1, ..., y_n\}$. In this case $L_G(B)$ is the totality of all elements of the form $f + \sum_{i=1}^{n} g_i y_i$ as f ranges over F and the g_i's over G.

A concept which will prove useful in the next section is that of a substitution. Intuitively speaking, we substitute an element of $L_G(B)$ for every occurrence of y_j in an algorithm, and thus obtain a new algorithm. The multiplicative complexity of the quantities computed by this new algorithm may be easier to estimate. Since the processof computation may involve division, special care has to be taken that we do not divide by 0.

DEFINITION 5. A substitution is a mapping $\alpha: \{y_1, ..., y_n\} \to L_G(B)$, that is, α is a mapping satisfying $\alpha(y_i) = f_i + \sum_{j=1}^{n} g_{i,j} y_j$ where $f_i \in F$ and $g_{i,j} \in G$. This mapping can be extended uniquely to a homomorphism $\bar{\alpha}: F[y_1, ..., y_n] \to F[y_1, ..., y_n]$, which leaves every $f \in F$ fixed. (Note that $\bar{\alpha}$ leaves $L_G(F)$ invariant.) We can further extend $\bar{\alpha}$ to a partial mapping $\alpha^*: F(y_1, ..., y_n) \to F(y_1, ..., y_n)$ defined by $\alpha^*(a/b) = \bar{\alpha}(a)/\bar{\alpha}(b)$ $(a, b \in F[y_1, ..., y_n]$ whenever $\bar{\alpha}(b) \neq 0$.

DEFINITION 6. A substitution α is said to be a *specialization of* y_k if $\alpha(y_j) = y_j$ for $j \neq k$, and $\alpha(y_k) = f + \sum_{i \in I} g_i y_i$ for some $f \in F$, $g_i \in G$, where $I = \{1, 2, ..., n\} - \{k\}$. A substitution α is said to be a *specialization* if α is a specialization of y_k for some k.

DEFINITION 7. A substitution α is said to be *compatible with an algorithm* $\mathscr{A}$ if every step of $\mathscr{A}$ is in the domain of α^*. A substitution α is said to be *compatible with* $\{\psi_1, ..., \psi_t\}$ if it is compatible with some algorithm $\mathscr{A}$ computing $\{\psi_1, ..., \psi_t\}$ such that $\mu(\mathscr{A}) = \mu(\psi_1, ..., \psi_t)$. (In particular, it follows that $\psi_1, ..., \psi_t$ are all in the domain of α^*.)

LEMMA 4. *Let* α *be a substitution compatible with* $\{\psi_1, ..., \psi_t\}$. *For every algorithm* $\mathscr{A}$ *computing* $\{\psi_1, ..., \psi_t\}$ *such that* α *is compatible with* $\mathscr{A}$ *there exists an algorithm* $\mathscr{A}'$ *computing* $\{\alpha^*(\psi_1), ..., \alpha^*(\psi_t))$ *such that* $\mu(\mathscr{A}') \leqslant \mu(\mathscr{A})$. *Furthermore,*

$$\mu_B(\alpha^*(\psi_1), ..., \alpha^*(\psi_t)) \leqslant \mu_B(\psi_1, ..., \psi_t).$$

Proof. Let $\mathscr{A}$ be the algorithm of the lemma. Since $B = F \cup \{y_1, \ldots, y_n\}$, then $h_s \in B$ if and only if $h_s = y_j$ for some j or $h_s = f$ for some $f \in F$. Replacing each step h_s of $\mathscr{A}$ by the sequence of non m/d steps computing $\alpha^*(h_s)$, and replacing each step $h_s = h_k \circ h_l$ $(k, l < s)$, where $\circ$ is one of the field operations, by $\alpha^*(h_s) = \alpha^*(h_k) \circ \alpha^*(h_l)$, we obtain the algorithm $\mathscr{A}'$, which computes $\alpha^*(h_s)$ for every $h_s \in \mathscr{A}$. In particular $\mathscr{A}'$ computes $\{\alpha^*(\psi_1), \ldots, \alpha^*(\psi_t)\}$. The only m/d steps of $\mathscr{A}'$ are those obtained as replacements of m/d steps of $\mathscr{A}$. (It should be emphasized that a replacement of an m/d step of $\mathscr{A}$ is not necessarily an m/d step of $\mathscr{A}'$, but that a replacement of non-m/d steps of $\mathscr{A}$ must contain only non-m/d steps of $\mathscr{A}'$.) Therefore $\mu(\mathscr{A}') \leqslant \mu(\mathscr{A})$. The second half of the lemma is proved by choosing $\mathscr{A}$ such that $\mu(\mathscr{A}) = \mu_B(\psi_1, \ldots, \psi_t)$.

LEMMA 5. *Let α be a substitution compatible with $\{\psi_1, \ldots, \psi_t\}$ such that $\alpha^*(\psi_i) \in L_G(B)$ for $i = 1, 2, \ldots, k$. Then $\mu_B(\alpha^*(\psi_{k+1}), \ldots, \alpha^*(\psi_t)) \leqslant \mu_B(\psi_1, \ldots, \psi_t) - d(k)$, where $d(k)$ is the dimension of $L_G(r(\psi_1), \ldots, r(\psi_k))$.*

Proof. By assumption α is compatible with an algorithm $\mathscr{A}$ computing $\{\psi_1, \ldots, \psi_t\}$ such that $\mu(\mathscr{A}) = \mu_B(\psi_1, \ldots, \psi_t)$. By Corollary 2 there exists an algorithm (over $B' = B \cup \{\psi_1, \ldots, \psi_k\}$) such that $\mu(\mathscr{A}') \leqslant \mu_B(\psi_1, \ldots, \psi_t) - d(k)$. An examination of the construction of Lemma 1 which leads to $\mathscr{A}'$ shows that since all the steps of $\mathscr{A}$ are in the domain of α^* so are all the steps of $\mathscr{A}'$. We apply the construction of Lemma 4 to $\mathscr{A}'$, which is possible because $\alpha^*(\psi_i) \in L_G(B)$ for $i = 1, 2, \ldots, k$, so $\alpha^*(B') \subseteq L_G(B)$. The resulting algorithm $\mathscr{A}''$ is over B, and since $\mu(\mathscr{A}'') \leqslant \mu(\mathscr{A}')$, we have proved the lemma.

A special situation arises when the $\psi_1, \psi_2, \ldots, \psi_k$ are of the special form $\psi_i = f_i \cdot y$ $(i = 1, 2, \ldots, k)$, where $f_i \in F$ and $y \in \{y_1, y_2, \ldots, y_n\}$. The following lemma guarantees the existence of a substitution (in fact a specialization) α which satisfies the condition of Lemma 5.

LEMMA 6. *Let G have infinitely many elements. If $\psi_i = f_i \cdot y$, $f_i \in F$, $y \in \{y_1, \ldots, y_n\}$ $(i = 1, 2, \ldots, k)$ then there exists a specialization α of y compatible with $\{\psi_1, \psi_2, \ldots, \psi_t\}$ such that $\mu_B(\alpha^*(\psi_{k+1}), \ldots, \alpha^*(\psi_t)) \leqslant \mu_B(\psi_1, \psi_2, \ldots, \psi_t) - d(k)$ where $d(k)$ is the dimension of $L_G(r(\psi_1), \ldots, r(\psi_k))$.*

Proof. We may with no loss of generality assume $y = y_1$. Let $\mathscr{A}$ be an algorithm computing $\{\psi_1, \psi_2, \ldots, \psi_t\}$ such that $\mu(\mathscr{A}) = \mu(\psi_1, \ldots, \psi_t)$. Every step h_i of $\mathscr{A}$ can be written as $h_i = a_i/b_i$ where $a_i, b_i \in F[y_1, \ldots, y_n] = F[y_2, \ldots, y_n][y_1]$. As $\mathscr{A}$ has finitely many steps, and since every b_i (viewed as a polynomial in y_1) has finitely many roots in $F[y_2, \ldots, y_n]$, there are only a finite set X of elements of $F[y_2, \ldots, y_n]$ which are roots of some b_i. Because G has infinitely many elements, there exists a $g \in G$ such that $g \notin X$. Let α be a specialization of $y = y_1$ defined by $\alpha(y_1) = g$, $\alpha(y_i) = y_i$ for $i \neq 1$. By construction, α is compatible with $\{\psi_1, \ldots, \psi_t\}$ and $\alpha^*(\psi_i) = f_i \cdot g \in L_G(B)$ for $i = 1, 2, \ldots, k$. Applying Lemma 5 to this α we obtain the desired result.

Remark 3. We can replace y in Lemma 6 by any non-zero element z of $L_G(\{y_1,\ldots,y_n\})$. In this case, α can be chosen to be a specialization of any y_i which has a non-zero coefficient in z.

The following lemma guarantees the existence of a substitution which reduces the multiplicative complexity by at least 1. Moreover, it assures us that this substitution is a specialization.

LEMMA 7. *Let G have infinitely many elements, and let $\{\psi_1,\ldots,\psi_t\}$ be such that $\mu_B(\psi_1,\ldots,\psi_t) \geqslant 1$. There exists a specialization α compatible with $\{\psi_1,\psi_2,\ldots,\psi_t\}$ satisfying*

$$\mu_B(\alpha^*(\psi_1),\ldots,\alpha^*(\psi_t)) \leqslant \mu_B(\psi_1,\ldots,\psi_t) - 1.$$

Proof. Let $\mathscr{A}$ be an algorithm for computing $\{\psi_1,\psi_2,\ldots,\psi_t\}$ satisfying $\mu(\mathscr{A}) = \mu_B(\psi_1,\ldots,\psi_t)$. Let h_s be the first m/d step of $\mathscr{A}$. By Remark 1, every step h_k of $\mathscr{A}$ for $k < s$ is in $L_G(B)$ and therefore is of the form $f + \sum_{i=1}^{n} g_i y_i$. As h_s is an m/d step, it can be written as either $h_s = h_k \cdot h_l$ $(k, k < s)$ or $h_s = h_k : h_l$ $(k, l < s)$. Let $h_k = f + \sum_{i=1}^{n} g_i y_i$ and $h_l = f' + \sum_{i=1}^{n} g_i y_i$. Since h_s is an m/d step either $h_l \notin F$, or if $h_l \in F$ then $h_k \notin F$. Assume $h_l \notin F$. (If $h_l \in F$ then $h_k \notin F$ and the same argument applies.) Let y be any of the y_i's which has a non-zero coefficient in h_l. Assume $y = y_1$. For each $g \in G$ there exists a specialization α of y_1 such that $g_1\alpha(y_1) = g - f' - \sum_{i=2}^{n} g_i^1 y_i$, and $\alpha(y_j) = y_j$, $j = 2,\ldots,n$.

Assume $g \in G$ is chosen so that the α so constructed is compatible with $\mathscr{A}$. Applying the construction of Lemma 4 to $\mathscr{A}$ we obtain an algorithm $\mathscr{A}'$. Every non-m/d step of $\mathscr{A}$ remains a non-m/d step of $\mathscr{A}'$. In addition, the step h_s of $\mathscr{A}$ becomes $\alpha^*(h_s) = \alpha^*(h_k) \cdot g \in L_G(B)$, so $\mathscr{A}'$ has at least one m/d step fewer than $\mathscr{A}$. Consequently, $\mu_B(\alpha^*(\psi_1),\ldots,\alpha^*(\psi_t)) \leqslant \mu(\mathscr{A}') \leqslant \mu(\mathscr{A}) - 1 = \mu_B(\psi_1,\ldots,\psi_t) - 1$.

To finish this proof, we have to show the existence of an α compatible with $\mathscr{A}$. As in the proof of Lemma 6, we write each step h_i of $\mathscr{A}$ as $h_i = a_i/b_i$ where $a_i, b_i \in F[y_1,\ldots,y_n] = F[y_2,\ldots,y_n][y_1]$. The set X of elements of $F[y_2,\ldots,y_n]$ which are roots of some b_i is finite, and, since G has infinitely many elements there exists a $g \in G$ such that $(g - f' - \sum_{i=1}^{n} g_i y_i)/g_1^1$ is not an element of X. Therefore the α constructed using this g is compatible with $\mathscr{A}$. This proves the lemma.

Of special interest are the elements $\psi_i \in H$ which are linear in the y_j's. That is, the elements to be computed are $\psi_i = \sum_{j=1}^{n} f_{i,j} y_j$, for some $f_{i,j} \in F$. We denote by $\mathbf{f}_i \in F^n$ the vector whose components are $f_{i,1}, f_{i,2},\ldots,f_{i,n}$; and by $\mathbf{y}$ the vector whose components are $y_1, y_2,\ldots,y_n$. We denote ψ_i by $(\mathbf{f}_i, \mathbf{y})$.

Let $\psi_1 = (\mathbf{f}_1, \mathbf{y})$ and $\psi_2 = (\mathbf{f}_2, \mathbf{y})$ be such that $\mathbf{f}_1 - \mathbf{f}_2 \in G^n$. Since $B = F \cup \{y_1,\ldots,y_m\}$ it follows that $r(\psi_1 - \psi_2) = 0$. In fact, $r(\psi_1 - \psi_2) = 0$ if and only if $\mathbf{f}_1 - \mathbf{f}_2 \in G^n$. This observation motivates our viewing F as a vector space over G, and defining $\bar{F}$ as the quotient space $\bar{F} = F/G$. We will use ρ to

denote the natural homomorphism $\rho: F \to \bar{F}$. The mapping ρ can be extended in a natural way to a homomorphism $F^m \to \bar{F}^m$ for every m. By abuse of notation, we will also use ρ to denote this extended mapping.

Remark 4. If $\psi_i = (\mathbf{f}_i, \mathbf{y})$, $i = 1, 2, \ldots, t$ then the dimension of $L_G(r(\psi_1), \ldots, r(\psi_t))$ is the same as the dimension of $L_G(\rho(\mathbf{f}_1), \ldots, \rho(\mathbf{f}_t))$.

DEFINITION 8. Let α be the substitution $\alpha(y_i) = f_i + \sum_{j=1}^{n} g_{i,j} y_j$. The *homogeneous part of* α is the substitution α' defined by $\alpha'(y_i) = \sum_{j=1}^{n} g_{i,j} y_j$. If $\alpha = \alpha'$ then α is called homogeneous.

Remark 5. Let $\psi_i = (\mathbf{f}_i, \mathbf{y})$, $i = 1, 2, \ldots, t$ and let α and β be two substitutions with the same homogeneous parts then $r(\alpha^*(\psi_i)) = r(\beta^*(\psi_i))$. Consequently the choice of $g \in G$ in the proofs of Lemma 6 and Lemma 7, which does not affect the homogeneous part of the α, does not affect the multiplicative complexity of the $\alpha^*(\psi_i)$'s.

LEMMA 8. *Let F have infinitely many elements, then for every homogeneous substitution α there exists a substitution β whose homogeneous part is α, such that β is compatible with $\{\psi_1, \ldots, \psi_t\}$.*

Proof. Let $\mathscr{A}$ be an algorithm $(h_1, h_2, \ldots, h_s)$ which computes $\{\psi_1, \psi_2, \ldots, \psi_t\}$ and such that $\mu(\mathscr{A}) = \mu_B(\psi_1, \ldots, \psi_t)$. Let $h_i = a_i/b_i$, $a_i, b_i \in F[y_1, \ldots, y_n]$. We want to show that there exists a substitution β whose homogeneous part is α such that $\beta^*(b_i) \neq 0$ for $i = 1, 2, \ldots, s$. The following lemma implies the existence of such a β.

LEMMA 8'. *Let F be a field, F' a subset of F with infinite cardinality, $\{y_1, \ldots, y_n\}$ and $\{z_1, \ldots, z_m\}$ two sets of distinct indeterminates, and $\{b_1, b_2, \ldots, b_t\}$ a finite set of non-zero elements of $F[y_1, \ldots, y_n]$. Let α be a mapping $\alpha: \{y_1, \ldots, y_n\} \to F(z_1, \ldots, z_m)$ which is extended to a mapping $\bar{\alpha}: F[y_1, \ldots, y_n] \to F(z_1, \ldots, z_m)$ leaving every $f \in F$ fixed. There exists a mapping $\beta: \{y_1, \ldots, y_n\} \to F(z_1, \ldots, z_m)$ such that for $i = 1, 2, \ldots, n$, $\beta(y_i) - \alpha(y_i) \in F'$, and $\bar{\beta}(b_j) \neq 0$, $j = 1, 2, \ldots, t$.*

Proof. Let n be the number of y_i's. We will prove the lemma by induction on n. If $n = 1$ each b_j is a polynomial in y_i with coefficients in F. (Note that if b_j is constant then it is not zero.) Therefore b_j has only a finite number of roots. Consequently, the set X of all roots of all the b_j's is finite, and there exists an $f \in F'$ such that $\alpha(y_1) + f \notin X$. The mapping $\beta(y_1) = \alpha(y_1) + f$ satisfies the condition of the lemma. Assume the lemma proved for $n \leq k$, we will prove it for $n = k + 1$. Since $F[y_1, \ldots, y_{k+1}] = F[y_1, \ldots, y_k][y_{k+1}]$ every b_j is a polynomial in y_{k+1} with coefficients in $F[y_1, \ldots, y_k]$. Let $J \subseteq \{1, 2, \ldots, t\}$ be the set of indices j such that $b_j \in F[y_1, \ldots, y_k]$, and $\{c_1, c_2, \ldots, c_s\} \subseteq F[y_1, \ldots, y_k]$ be the set of leading coefficients of the b_j's for $j \notin J$. Denoting by α' the restriction of α to $\{y_1, \ldots, y_k\}$ then by induction hypothesis there exists β' such that $\beta'(y_i) - \alpha'(y_i) \in F'$ for $i = 1, 2, \ldots, k$ and such that $\bar{\beta}'(y_j) \neq 0$ for $j \in J$

and $\bar{\beta}'(c_j) \neq 0$ for $j = 1, 2, \ldots, s$. $\bar{\beta}'$ can be extended to a mapping $\bar{\beta}': F[y_{k+1}][y_1, \ldots, y_k] \to F[z_1, \ldots, z_m][y_{k+1}]$ leaving y_{k+1} fixed. Let $\{b_1, b_2, \ldots, b_t\}$ be the images of $\{b_1', b_2', \ldots, b_t'\}$ under $\bar{\beta}'$. By the same argument as before there exists $f \in F'$ such that $\alpha(y_{k+1}) + f$ is not a root of any b_j' $(j = 1, 2, \ldots, t)$. The mapping β, defined by $\beta(y_j) = \beta'(y_j)$, $\beta(y_{k+1}) = \alpha(y_{k+1}) + f'$ satisfies the conclusion of the lemma.

To finish the proof of Lemma 8, let γ be the isomorphism $\gamma: F[y_1, \ldots, y_n] \to F[z_1, \ldots, z_n]$ which leaves every $f \in F$ fixed and maps each y_j into z_j $(j = 1, 2, \ldots, n)$. Choose α_1 in Lemma 8' as $\gamma\alpha$, then by Lemma 8' there exists a β_1 such that $\beta_1(y_j) - \alpha_1(y_j) \in F$ and $\bar{\beta}_1(b_i) \neq 0$, $i = 1, 2, \ldots, s$. The mapping $\beta = \gamma^{-1}\beta_1$ satisfies the condition of Lemma 8.

COROLLARY 4. *Let F have infinitely many elements, and let $\psi_i = (\mathbf{f}_i, \mathbf{y})$ $(i = 1, 2, \ldots, t)$. Let α be a substitution such that the matrix $(g_{i,j})$ defining its homogeneous part is invertible. Then there exists a substitution β whose homogeneous part is defined by $(g_{i,j})^{-1}$, and consequently $r(\beta^*\alpha^*(\psi)_i)) = r(\psi_i)$. Therefore,*

$$\mu_B(\alpha^*(\psi_1), \ldots, \alpha^*(\psi_t)) = \mu_B(\psi_1, \ldots, \psi_t).$$

In this paper we are considering algorithms which include the operation of division. The inclusion of division affected some of the results which would have be strengthened otherwise. We indicate the nature of these results.

DEFINITION 1'. Let G be a field, F a ring (with identity) which includes G, and let $H = F[y_1, \ldots, y_n]$. Let B be a subset of H. A *division-free algorithm* $\mathscr{A}$ is a finite sequence $(h_1, h_2, \ldots, h_s)$ of elements of H, which are called steps of $\mathscr{A}$, such that for each h_i either $h_i \in B$ or $h_i = h_k \circ h_l$ for some $k, l < i$, where $\circ$ stands for $+$, $-$, or $\times$. $\mathscr{A}$ is said to compute $\{\psi_1, \ldots, \psi_t\} \subseteq H$ if for each there exists a j such that $\psi_i = h_j$.

Remark 6. We can modify Definition 2 and 3 in a straightforward manner to the case of division-less algorithms.

Remark 7. If we had dealt with division-less algorithms then α^* would be a total mapping, and therefore compatible with all algorithms and all $\psi_i \in H$. Consequently we would have dropped the requirement that G has infinitely many elements which appear in Lemma 6, Lemma 7, and that F is infinite in Lemmas 8, 8' and Corollary 4. We could also have dropped the constraint that $\psi_i = (\mathbf{f}_i, \mathbf{y})$ which appears in Corollary 4.

III. THE MAIN RESULT

Let $R(u) = \sum_{i=0}^{n-1} f_i u^i$ be a polynomial with coefficients in F, $S(u) = \sum_{i=0}^{n-1} h_i u^i$ be a polynomial with coefficients in H, and $P(u) = u^n + \sum_{i=0}^{n-1} g_i u^i$ be a monic

polynomial with coefficients in G. The set of coefficients of the polynomial $T(u) = R(u) \cdot S(u) \bmod P(u)$ will be denoted by $C(P; \mathbf{f}, \mathbf{h})$, where $\mathbf{f}$ is the vector of coefficients of $R(u)$, and $\mathbf{h}$ the vector of coefficients of $S(u)$. More generally, let $R_i(u)$ be a polynomial of degree $n_i - 1$ with coefficients in F $(i = 1, 2, \ldots, s)$, $S_i(u)$ be a polynomial of degree $n_i - 1$ with coefficients in H $(i = 1, 2, \ldots, s)$, and $P_i(u)$ be a monic polynomial of degree n_i with coefficients in H $(\ = 1, 2, \ldots, s)$. We will denote the set of coefficients of all the polynomials $T_i(u) = R_i(u) \cdot S_i(u) \bmod P_i(u)$ $(\ = 1, 2, \ldots, s)$ by $\{C(P_i ; \mathbf{f}_i , \mathbf{h}_i)\}$. In the special case that all the coefficients of all the $S_i(u)$'s are distinct indeterminates we will denote it by $\{C(P_i ; \mathbf{f}_i , \mathbf{y}_i)\}$. The main result is a lower bound on the multiplicative complexity $\mu_B(\{C(P_i ; \mathbf{f}_i , \mathbf{y}_i)\})$ in the case that all the $P_i(u)$'s are irreducible polynomials (over G). As was mentioned in the previous section, we assume $B = F \cup \{y_1, \ldots, y_n\}$. By the Chinese Remainder Theorem this will also yield a lower bound in the case that none of the $P_i(u)$'s has repeated roots.

To apply the results of the previous section to estimating the multiplicative complexity of $\{C(P_i ; \mathbf{f}_i , y_i)\}$ we need to investigate the dimension of $L_G(r(\{C(P_i ; \mathbf{f}_i , \mathbf{h}_i)\}))$, where each of the coordinates of the $\mathbf{h}_i$'s lies in $L_G(\{\mathbf{y}_i\})$ the linear span (over G) of all the indeterminates.

In the following it will be convenient not to distinguish between a vector and the set of its coordinates. Thus, if $\mathbf{f} \in F^n$ is a vector with coordinates $f_0 , f_1 , \ldots, f_{n-1}$, we will denote the linear span (over G) of $f_0 , f_1 , \ldots, f_{n-1}$ by $L_G(\mathbf{f})$, and denote the set $\{\rho(f_0), \rho(f_1), \ldots, \rho(f_{n-1})\}$ by $\rho(\mathbf{f})$.

LEMMA 9. *Let $P(u)$ be a monic irreducible polynomial (over G) of degree n, and let $\mathbf{g} \in G^n$ be a non-zero vector, then $L_G(\mathbf{f}) = L_G(C(P; \mathbf{f}, \mathbf{g}))$.*

Proof. Let A be the companion matrix of $P(u)$. Then viewing $C(P; \mathbf{f}, \mathbf{g})$ as a vector we have $C(P; \mathbf{f}, \mathbf{g}) = (\sum_{i=0}^{n-1} f_i A^i)\, \mathbf{g}$, where the operation in the bracket is in the algebra of matrices. Because polynomial multiplication is commutative, we also have $C(P; \mathbf{f}, \mathbf{g}) = (\sum_{i=0}^{n-1} g_i A^i)\, \mathbf{f}$. Since $P(u)$ is an irreducible polynomial of degree n, the matrix $\sum_{i=0}^{n-1} g_i A^i$ is non-singular. Consequently, the set $\{\mathbf{v} \cdot \sum_{i=0}^{n-1} g_i A^i\}$ as $\mathbf{v}$ ranges over all (row) vectors in G^n, is G^n. But $L_G(\mathbf{f}) = \{\mathbf{v} \cdot \mathbf{f} \mid \mathbf{v} \in G^n\}$, and $L_G(C(P; \mathbf{f}, \mathbf{g})) = \{\mathbf{v} \cdot (\sum_{i=0}^{n-1} g_i A^i)\, \mathbf{f} \mid \mathbf{v} \in G^n\} = L_G(\mathbf{f})$.

COROLLARY 5. *Let $P(u)$ and $\mathbf{g}$ be as in Lemma 8, then $L_G(\rho(\mathbf{f})) = L_G(\rho(C(P; \mathbf{f}, \mathbf{g})))$.*

COROLLARY 6. *If all the $P_i(u)$'s are irreducible polynomials $(i = 1, 2, \ldots, s)$ and all the $\mathbf{g}_i$'s are non-zero vectors with coefficients in G, then*

$$L_G(\rho(\{f_i\})) = L_G(\rho(\{C(P_i ; \mathbf{f}_i , \mathbf{g}_i)\})).$$

Combining Corollary 6 and Remark 4 we obtain:

COROLLARY 7. *Let $P_i(u)$ and $\mathbf{g}_i$ be as in Corollary* 6, *and let $\mathbf{h}_i = \mathbf{g}_i y$ (y an indeterminate) then the dimension of $L_G(r(\{C(P_i\,;\mathbf{f}_i\,,\mathbf{h}_i)\}))$ is the same as the dimension of $L_G(\rho(\{\mathbf{f}_i\}))$.*

Remark 8. We can replace the indeterminate y in Corollary 8 by any non-zero linear combination (over G) of the indeterminates.

COROLLARY 8. *Let P be an irreducible polynomial of degree n, $\mathbf{f} \in F^n$ be such that dimension of $L_G(\rho(\mathbf{f}))$ is positive, and $\mathbf{h} \in (L_G(y_1\,,\ldots,\,y_m))^n$ (m not necessarily the same as n) such that the dimension of $L_G(\mathbf{h})$ is positive, then dimension of $L_G(r(C(P;\mathbf{f},\mathbf{h})))$ is positive and by Remark* 1, $\mu_B(C(P;\mathbf{f},\mathbf{h})) \geqslant 1$.

Proof. Let $z_1\,, z_2\,,\ldots, z_s \in L_G(y_1\,,\ldots,\,y_m)$ be linearly independent and such that $L_G(z_1\,,\ldots,\,z_s) = L_G(\mathbf{h})$. There exist non-zero vectors $\mathbf{g}_1\,, \mathbf{g}_2\,,\ldots,\, \mathbf{g}_s \in G^n$ such that $\mathbf{h} = \sum_{i=1}^{s} g_i z_i$ and therefore $C(P;\mathbf{f},\mathbf{h}) = \sum_{i=1}^{s} C(P;\mathbf{f},g_i z_i)$. The dimension of $L_G(r(C(P;\mathbf{f},\mathbf{h})))$ is 0 if and only if for all $i = 1, 2,\ldots, s$ the dimension of $L_G(r(C(P;\mathbf{f},g_i z_i)))$ is 0. But by Corollary 7 none of the dimensions of $L_G(r(C(P;\mathbf{f},g_i z_i)))$ is 0. This proves the Corollary.

LEMMA 10. *Let P be an irreducible polynomial of degree n, and let $\mathbf{f} \in F^n$ be such that the dimension of $L_G(\rho(\mathbf{f}))$ is positive. If $\mathbf{y}$ be the vector whose coordinates are the distinct indeterminates $y_1\,, y_2\,,\ldots, y_n$, then the dimension of $L_G(r(C(P;\mathbf{f},\mathbf{y})))$ is n.*

Proof. Let A be the companion matrix of P, and let $f_0\,, f_1\,,\ldots, f_{n-1} \in F$ be the coordinates of $\mathbf{f}$. Since $C(P;\mathbf{f},\mathbf{y}) = (\sum_{i=0}^{n-1} f_i A^i)\,\mathbf{y}$, we have to prove, by Remark 4, that for no non-zero row vector $\mathbf{v} \in G^n$ is $\mathbf{v}(\sum_{i=0}^{n-1} f_i A^i) \in G^n$.

Let K be a non-singular matrix with entries in G such that $A^T = KAK^{-1}$. Then $\mathbf{v}\sum_{i=0}^{n-1} f_i A^i = \mathbf{v}\sum_{i=0}^{n-1} f_i (K^{-1}A^T K)^i = (\mathbf{v}K^{-1})(\sum_{i=0}^{n-1} f_i (A^T)^i)\,K$. Let $\mathbf{v}K^{-1}$ be the row vector $\mathbf{u} = (u_0\,, u_1\,,\ldots, u_{n-1})$, then $\mathbf{v}(\sum_{i=0}^{n-1} f_i A^i) = (\mathbf{u}\sum_{i=0}^{n-1} f_i (A^T)^i)\,K^{-1}$. But $\mathbf{u}\sum_{i=0}^{n-1} f_i (A^T)^i$ is the row vector (in F^n) whose coordinates are the coefficients of the polynomial $(\sum_{i=0}^{n-1} u_i w^i)(\sum_{i=0}^{n-1} f_i w^i)$ mod P. Since polynomial multiplication is commutative, we obtain that $\mathbf{u}\sum_{i=0}^{n-1} f_i (A^T)^i = \mathbf{f}\sum_{i=0}^{n-1} u_i (A^T)^i$. Assume $\mathbf{v}(\sum_{i=0}^{n-1} f_i A^i) = \mathbf{g} \in G^n$, then $\mathbf{f}\sum_{i=0}^{n-1} u_i (A^T)^i = K^{-1}\mathbf{g}$ is also in G^n. Because $\mathbf{v} \neq 0$ then $\mathbf{u} = \mathbf{v}K^{-1} \neq 0$. Since P is an irreducible polynomial of degree n, the matrix $\sum_{i=0}^{n-1} u_i (A^T)^i$ is non-singular, and therefore $\mathbf{f} = (\sum_{i=0}^{n-1} u_i (A^T)^i)^{-1}\,K^{-1}\mathbf{g}$ is also in G^n contradicting the assumption that the dimension of $L_G(\rho(\mathbf{f}))$ is positive. This proves the lemma.

COROLLARY 9. *Let P_i be an irreducible polynomial of degree n_i ($i = 1, 2,\ldots, s$), let $\mathbf{f}_i \in F^n$. be such that dimension of $L_G(\rho(\mathbf{f}_i))$ is positive ($i = 1, 2,\ldots, s$), and let $\mathbf{y}_i$ be a vector of n_i coordinates each an indeterminate ($i = 1, 2,\ldots, s$). If all the indeterminates in the set $\{\mathbf{y}_i\}$ are distinct then the dimension of $L_G(r(\{C(P_i\,;\mathbf{f}_i\,,\mathbf{y}_i)\}))$ is $\sum_{i=1}^{s} n_i$.*

Before proving the main theorem we need one more lemma.

LEMMA 11. *Let* $\mathbf{h}$ *be a vector whose coordinates are in* $L_G(y_1, y_2, \ldots, y_m)$, *and let* α *be a specialization, then* $\dim L_G(\alpha^*(\mathbf{h})) \geqslant \dim L_G(\mathbf{h}) - 1$.

Proof. Let M be a matrix with entries in G such that $\mathbf{h} = M\mathbf{y}$, where $\mathbf{y}$ is the vector $(y_1, y_2, \ldots, y_m)$. Then $\dim L_G(\mathbf{h}) = \text{Rank}(M)$. Since α is a specialization, then $\alpha(\mathbf{y}) = N\mathbf{y}$ where $N = I + T$, I the identity matrix and T a matrix of rank 1. As $\alpha^*(\mathbf{h}) = M \cdot N\mathbf{y}$ we obtain that $\dim L_G(\alpha^*(\mathbf{h})) = \text{Rank}(M \cdot N) = \text{Rank}(M \cdot (I + T)) = \text{Rank}(M + MT) \geqslant \text{Rank}(M) - \text{Rank}(MT) \geqslant \dim L_G(\mathbf{h}) - 1$.

THE MAIN THEOREM. *Let* P_i *be an irreducible polynomial of degree* n_i $(i = 1, 2, \ldots, s)$, *let* $f_i \in F^n$. *be a vector such that* $\dim L_G(\mathbf{f}_i) \geqslant 1$ $(i = 1, 2, \ldots, s)$, *and let* $\mathbf{y}_i$ *be a vector of* n_i *distinct indeterminates* $(i = 1, 2, \ldots, s)$ *such that all the indeterminates in all the* $\mathbf{y}_i$*'s are distinct. Let* $\{\mathbf{f}_i\}$ *denote the set of all the coordinates of all the* $\mathbf{f}_i$*'s and* $k = \dim L_G(\rho(\{\mathbf{f}_i\}))$. *Then* $\mu_B(\{C(P_i ; \mathbf{f}_i, y_i)\}) \geqslant k - s + \sum_{i=1}^{s} n_i = \dim L_G(\rho(\{\mathbf{f}_i\})) + \sum_{i=1}^{s} (\deg P_i - 1)$.

Proof. The proof will proceed by repeatedly applying the specializations of Lemmas 6 and 7, reducing the multiplicative complexity. This will be done until the application of the composite substitution to $\{C(P_i ; \mathbf{f}_i, \mathbf{y}_i)\}$ will yield elements of $L_G(B)$, i.e., quantities whose multiplicative complexity is 0. A count of the reduction in the multiplicative complexity guaranteed by Lemmas 6 and 7 will yield the theorem.

Since Lemmas 6 and 7 assume that G has infinitely many elements, we will assume, at first, that the cardinality of G is infinite, and relax this assumption at the end of the proof.

Each $C(P_i ; \mathbf{f}_i, \mathbf{y}_i)$ satisfies the conditions of Corollary 8, so we obtain that $\mu_B(\{C(P_i ; \mathbf{f}_i, \mathbf{y}_i)\}) \geqslant 1$, and Lemma 7 guarantees the existence of a specialization α_1, such that

$$\mu_B(\alpha_1^*(\{C(P_i ; \mathbf{f}_i, \mathbf{y}_i)\})) \leqslant \mu_B(\{C(P_i ; \mathbf{f}_i, \mathbf{y}_i)\}) - 1.$$

By Remark 5 we may take α_1 to be a homogeneous specialization. Since, for any substitution α, $\alpha^*(\{C(P_i ; \mathbf{f}_i, \mathbf{y}_i)\}) = \{C(P_i ; \mathbf{f}_i, \alpha^*(y_i))\}$ we obtain that $\mu_B(\{C(P_i ; \mathbf{f}_i, \alpha_1^*(\mathbf{y}_i))\}) \leqslant \mu_B(\{C(P_i ; \mathbf{f}_i, \mathbf{y}_i)\}) - 1$. If for all $i = 1, 2, \ldots, s$, $\dim L_G(\alpha_1^*(\mathbf{y}_i)) > 1$ the condition of Corollary 8 and Lemma 7 are still satisfied by $\{C(P_i ; \mathbf{f}_i, \alpha_1^*(\mathbf{y}_i))\}$ and therefore there exists a specialization α_2 (which by Remark 5 may be taken to be homogeneous) which further reduces the multiplicative complexity by 1. That is, if $\beta_2 = \alpha_2 \cdot \alpha_1$ then $\mu_B(\{C(P_i ; \mathbf{f}_i, \beta_2^*(\mathbf{y}_i))\}) \leqslant \mu_B(\{C(P_i ; \mathbf{f}_i, \mathbf{y}_i)\}) - 2$. In general, we continue this process of obtaining specializations $\alpha_3, \alpha_4, \ldots, \alpha_l$ and substitution $\beta_3, \beta_4, \ldots, \beta_l$ defined by $\beta_{j+1} = \alpha_{j+1} \cdot \beta_j$ as long as for every $i = 1, 2, \ldots, s$ $\dim L_G(\beta_j^*(\mathbf{y}_i)) > 1$. Note that Lemma 11 guarantees that $\dim L_G(\beta_{j+1}^*(\mathbf{y}_i)) \geqslant \dim L_G(\beta_j^*(\mathbf{y}_i)) - 1$. Let l be

the smallest integer such that $\dim L_G(\beta_l^*(\mathbf{y}_i)) = 1$ for some $i \in \{1, 2, \ldots, s\}$. When this happens we stop the application of Lemma 7. (Note that if $n_i = 1$ for some i then $l = 0$, and we take β_l as the identity substitution.) So far we have obtained that $\mu_B(\{C(P_i ; \mathbf{f}_i , \beta_l^*(\mathbf{y}_i))\}) \leqslant \mu_B(\{C(P_i ; \mathbf{f}_i , \mathbf{y}_i)\}) - l$.

Let $i \in \{1, 2, \ldots, s\}$ be such that $\dim L_G(\beta_l^*(\mathbf{y}_i)) = 1$, i.e., $\beta_l^*(\mathbf{y}_i) = \mathbf{g} \cdot z_1$ for some non-zero $z_1 \in L_G(\{\mathbf{y}_i\})$, where g is a non-zero vector. Let $J_1 = \{i \mid \beta_l^*(\mathbf{y}_i) = \mathbf{g}_i \cdot z_1\}$ then by Lemma 6 (and Remark 3) there exists a specialization γ_1, which we may take to be homogeneous, such that $\mu_B(\{C(P_i \mathbf{f}_i , \gamma_1^* \beta_l^*(\mathbf{y}_i))\}) \leqslant \mu_B(\{C(P_i \mathbf{f}_i , \beta_l^*(\mathbf{y}_i))\}) - k_1$ where

$$k_1 = \dim L_G(r(\{C(P_i ; \mathbf{f}_i , \mathbf{g}_i \cdot z_1) \mid i \in J_1\})).$$

By Corollary 7 $k_1 = \dim L_G(\rho(\{\mathbf{f}_i \mid i \in J_1\}))$. Denoting $\gamma_1 \cdot \beta_l$ by β_{l+1} we obtain that

$$\mu_B(\{C(P_i ; \mathbf{f}_i , \beta_{l+1}^*(\mathbf{y}_i)) \mid i \notin J_1) \leqslant \mu_B(\{C(P_i ; \mathbf{f}_i , \mathbf{y}_i)\}) - l - k_1 .$$

If for all $i \notin J_1$ $\dim L_G(\beta_{l+1}^*(\mathbf{y}_i)) > 1$ we restart applying Lemma 7 and obtain $\alpha_{l+2}, \ldots, \alpha_{l+m+1}$, and $\beta_{l+2} = \alpha_{l+2} \cdot \beta_{l+1}, \ldots, \beta_{l+m+1} = \alpha_{l+m+1} \cdot \beta_{l+m}$ until for some $i \notin J_1$ $\dim L_G(\beta_{l+m+1}^*(y_i)) = 1$. (It can happen that $m = 0$.) We then define $J_2 = \{i \in J_1 \mid \beta_{l+m+1}(\mathbf{y}_i) = \mathbf{g}_i \cdot z_2\}$ for some non-zero $z_2 \in L_G(\{\mathbf{y}_i\})$. Using Lemma 6 we obtain a specialization γ_2 such that, denoting $\gamma_2 \cdot \beta_{l+m+1}$ by β_{l+m+2}, $\mu_B(\{C(P_i ; \mathbf{f}_i , \beta_{l+m+2}^*(y_i)) \mid i \notin J_1 \cup J_2\}) \leqslant \mu_B(\{C(P_i ; \mathbf{f}_i , \mathbf{y}_i)\}) - l - m - k_1 - k_2$, where $k_2 = \dim L_G(\rho(\{\mathbf{f}_i \mid i \in J_2\}))$. We continue to alternate between the applications of Lemma 7 and Lemma 6 until $J_1 \cup J_2 \cup \cdots = \{1, 2, \ldots, s\}$, (ending with the application of Lemma 6). Let $s' \leqslant s$ be the number of times Lemma 6 was applied. Let y be one of the indeterminates in $\mathbf{y}_i$, then, if none of the α_j's and γ_j's which are composed to make β_t is a specialization of y, $\dim L_G(\beta_t^*(\mathbf{y}_i)) \geqslant 1$, and by Corollary 8 $\mu_B(C(P_i ; \mathbf{f}_i , \beta_t^*(y_i))) \geqslant 1$. Thus, after the application of γ_s we must have used specializations of every single indeterminate in $\{\mathbf{y}_i\}$. That is, the otal number of applications of Lemmas 6 and 7 is $\sum_{i=1}^{s} n_i$, and therefore Lemma 7 was applied $(\sum_{i=1}^{s} n_i) - s'$ times. But when the process ends we have nothing to compute, hence $0 \leqslant \mu_B(\{C(P_i ; \mathbf{f}_i , \mathbf{y}_i)\}) - \sum_{i=1}^{s'} k_i - (\sum_{i=1}^{s} n_i - s')$, where $k_i = \dim L_G(\rho(\{\mathbf{f}_i \mid i \in J_i\}))$. But

$$\sum_{i=1}^{s'} k_i \geqslant \dim L_G(\{\mathbf{f}_i\}) = k,$$

and $s' \leqslant s$ so we obtain that

$$\mu_B(\{C(P_i ; \mathbf{f}_i , \mathbf{y}_i\}) \geqslant k - s + \sum_{i=1}^{s} n_i .$$

To finish the proof we have to relax the assumption that the cardinality of G is infinite. Assume G has a finite number of elements. Let y be an inde-

terminate not in any of the $\mathbf{y}_i$'s. Then replacing G by $G' = G(y)$ and F by $F' = F(y)$, we can view $\{C(P_i ; \mathbf{f}_i , \mathbf{y}_i)\}$ as a subset of $F'(\{\mathbf{y}_i\})$. Every algorithm $\mathscr{A}$ for computing $\{C(P_i ; \mathbf{f}_i , \mathbf{y}_i)\}$ over $F \cup \{\mathbf{y}_i\}$ is a-posteriori an algorithm over $F' \cup \{\mathbf{y}_i\}$. But G' has infinitely many elements and therefore $\mu(\mathscr{A}) \geqslant k - s + \sum_{i=1}^{s} n_i$. This proves the theorem.

COROLLARY 10. *Let cardinality of G be infinite. If* $\dim L_G(\{\mathbf{f}_i\}) = \sum_{i=1}^{s} n_i$ *then* $\mu_B(\{C(P_i ; \mathbf{f}_i , \mathbf{y}_i)\}) = 2\sum_{i=1}^{s} n_i - s$.

Proof. Substituting $\sum_{i=1}^{s} n_i$ for k in the main theorem we obtain inequality one way. The construction given in [1] shows that if G has enough elements then for any $\mathbf{f} \in F^n$, and irreducible polynomial P of degree n $\mu(C(P; \mathbf{f}_i , \mathbf{y}_i)) \leqslant 2n - 1$, and therefore the algorithm which computes each of the $C(P_i ; \mathbf{f}_i , \mathbf{y}_i)$ according to the construction of [1] satisfies $\mu(\mathscr{A}) = 2\sum_{i=1}^{s} n_i - s$. This proves the inequality the other way.

An examination of the proof of the main theorem shows that whenever $\dim L_G(\{\mathbf{f}_i\}) < \sum_{i=1}^{s} \dim L_G(\mathbf{f}_i)$ the statement of the theorem is not the best possible. For if $s' = s$ (we use the notation of the proof) each J_i is a singleton set and therefore we have shown that $\mu_B(\{C(P_i ; \mathbf{f}_i , \mathbf{y}_i)\} \geqslant \sum_{i=1}^{s} n_i + \sum_{i=1}^{s} \deg L_G(\mathbf{f}_i) - s$. If $s' < s$ then we can substitute $(s - 1)$ for s in the statement of the Theorem. Thus, for example, if $s = 2$ we obtain that $\mu_B(\{C(P_i ; \mathbf{f}_i , \mathbf{y}_i)) \geqslant m$ where $m = \min(n_1 + n_2 + \dim L_G(\{\mathbf{f}_i\}) - 1, n_1 + n_2 + \dim L_G(\mathbf{f}_1) + \dim L_G(\mathbf{f}_2) - 2)$.

Conjecture. Let P_i , $\mathbf{f}_i$, and $\mathbf{y}_i$ be as in the Main Theorem, then

$$\mu_B(\{C(P_i ; \mathbf{f}_i , \mathbf{y}_i)\}) \geqslant \sum_{i=1}^{s} (\deg P_i - 1) + \sum_{i=1}^{s} \dim L_G(\mathbf{f}_i).$$

The difference between the conjecture and what was proved in the Main Theorem is most pronounced when there exists an index i, or even a subset of the indices J, such that $L_G(\{\mathbf{f}_i \mid i \in J\}) \subseteq L_G(\{\mathbf{f}_i \mid i \notin J\})$. The following theorem, which slightly generalizes the Main Theorem, will be useful in dealing with the applications which have the condition described above.

THEOREM 1. *Let P_i , $\mathbf{f}_i$, and $\mathbf{y}_i$ $(i = 1, 2, \ldots, s)$ be as in the Main Theorem. Let J_1 , $J_2 \subseteq \{1, 2, \ldots, s\}$ be a partition of $\{1, 2, \ldots, s\}$, then*

$$\mu_B(\{C(P_i ; \mathbf{f}_i , \mathbf{y}_i)\}) \geqslant \sum_{i \in J} \deg P_i + \sum_{i \in J} (\deg P_i - 1) + \dim L_G(\{\mathbf{f}_i \, i \in J_2\}).$$

Proof. We will prove the theorem for the case that G has infinitely many elements. The agreement at the end of the proof of the Main Theorem shows that the conclusion of the theorem is also valid even for a finite G.

By Corollary 9, $\dim L_G(r(\{C(P_i ; \mathbf{f}_i , \mathbf{y}_i) \mid i \in J_1\})) = \sum_{i \in J_1} n_i$. Let α be the

homogeneous substitution $\alpha(\mathbf{y}_i) = 0$ for $i \in J_1$, $\alpha(\mathbf{y}_i) = \mathbf{y}_i$ for $i \in J_2$. By Lemma 8 there exists a substitution β, whose homogeneous part is α, which is compatible with $\{C(P_i ; \mathbf{f}_i , \mathbf{y}_i)\}$. For each $i \in J_1$ $C(P_i ; \mathbf{f}_i , \beta^*\mathbf{y}_i)) \subseteq L_G(B)$, and for each $i \in J_2$ $r(C(P_i ; \mathbf{f}_i , \beta^*(\mathbf{y}_i)) = r(C(P_i ; \mathbf{f}_i , \mathbf{y}_i))$. By Lemma 5 (and Corollary 9) $\mu_B(\{C(P_i ; \mathbf{f}_i , \mathbf{y}_i)\}) \geqslant \mu_B(\{C(P_i ; \mathbf{f}_i , \beta^*(\mathbf{y}_i)) \mid i \in J_2\}) + \sum_{i \in J_1} \deg P_i$. Applying the Main Theorem to $\mu_B(\{C(P_i ; \mathbf{f}_i , \mathbf{y}_i) \mid i \in J_2\})$ we obtain

$$\mu_B(\{C(P_i ; \mathbf{f}_i , \mathbf{y}_i)\}) \geqslant \sum_{i \in J_1} \deg P_i + \sum_{i \in J_2} (\deg P_i - 1) + \dim L_G(\{\mathbf{f}_i) \, i \in J_2\}).$$

Remark 9. Taking J_1 to be the empty set, Theorem 1 reduces to the Main Theorem.

IV. Applications

The Discrete Fourier Transform of n points, denoted by DFT(n), is a system of n forms $\overline{Y}_i = \sum_{i=0}^{n-1} w^{ij} y_j$ $(i = 0, 1, 2, \ldots, n-1)$ where w is the nth root of unity $w = e^{2\pi i/n}$. The computation of $\overline{Y}_0 = \sum_{j=0}^{n-1} y_i$ requires no m/d steps, and the coefficient of y_0 in the expression for $\overline{Y}_j$ is 1 for all j. Therefore studying the multiplicative complexity of DFT(n) it is sufficient to consider

$$Y_i = \sum_{j=1}^{n-1} w^{ij} y_j \qquad (i = 1, 2, \ldots, n-1).$$

We will consider first the case where $n = p$ is a prime number. Let M_p denote the group of positive integers smaller than p, with multiplication modulo p as the group operation. Consider the group algebra HM_p where $H = F(y_1, \ldots, y_{p-1})$ and F is some subfield of the complex numbers which includes the pth root of unity. Let $m_1 , m_2 , \ldots, m_{p-1}$ denote the elements of M_p (with $m_i \cdot m_j = m_k$ if and only if $i \cdot j = k \bmod p$). Consider the element $Y = \sum_{i=1}^{p-1} Y_i m_i \in HM_p$ defined by $Y = (\sum_{i=1}^{p-1} w^i \cdot m_i)(\sum_{i=1}^{p-1} y_i (m_i)^{-1})$. Each Y_i is a linear combination of the y_j's. The coefficient w^k of y_j in Y_i is determined by the k which satisfies $(m_k) \cdot (m_j)^{-1} = m_i$, that is, $m_k = m_i \cdot m_j$. That means that $k = i \cdot j \bmod p$, and since $w^p = 1$ we obtain that the coefficient of y_j in Y_i is w^{ij}. Therefore $Y_i = \sum_{j=1}^{p-1} w^{ij} y_j$ and we see that studying the multiplicative complexity of DFT(p) is the same as studying the multiplicative complexity of computing the coefficients of $(\sum_{j=1}^{p-1} w^i m_i)(\sum_{j=1}^{p-1} y_{\pi(i)} m_i)$ where $\pi(i) = j$ if $m_i = (m_j)^{-1}$.

The group M_p is isomorphic to the cyclic group Z_{p-1}. Let $1, u, u^2, \ldots, u^{p-2}$ denote the elements of Z_{p-1} $(u^{p-1} = 1)$, and let $t: M_p \to Z_{p-1}$ be an isomorphism. We denote by $y(i)$ the indeterminate y_j such that $t^{-1}(u^i) = m_k$ and $j = \pi(k)$. We denote by $w(i)$ the element w^j such that $m_j = t^{-1}(u^i)$, and by $Y(i)$ the element Y_j such that $m_j = t^{-1}(u^i)$. Using this notation we can express

the computation of DFT(p) as computing the coefficients of a product in the group algebra HZ_{p-1}. More precisely we obtain

$$\sum_{i=0}^{p-2} Y(i)\,u^i = \left(\sum_{i=0}^{p-2} w(i)\,u^i\right)\left(\sum_{i=0}^{p-2} y(i)\,u^i\right).$$

(This interpretation of computing DFT(p) as computing coefficients of the product of two elements in HZ_{p-1} was first given in [8]).

We can identify the group algebra HZ_{p-1} with the algebra $H[u]/\langle u^{p-1}-1\rangle$ of polynomials in u modulo the polynomial $u^{p-1}-1$. If we denote the polynomial $\sum_{i=0}^{p-2} w(i)\,u^i$ by $R(u)$, the polynomial $\sum_{i=0}^{p-2} y(i)\,u^i$ by $S(u)$, and the polynomial $\sum_{i=0}^{p-2} Y(i)\,u^i$ by $T(u)$, then $T(u) = R(u)\cdot S(u) \bmod u^{p-1}-1$. That is, using the notation of the previous section, computing the DFT(p) is the same as computing $C(u^{p-1}-1;\ \mathbf{w}(i),\ \mathbf{y}(i))$.

The polynomial $u^{p-1}-1$ is reducible (unless $p=2$), and the results of the previous section dealt with irreducible polynomials. The link which enables us to apply the results of the previous section to the computation of DFT(p) is the Chinese Remainder Theorem. For the sake of completeness we will state a version of the Chinese Remainder Theorem.

Chinese Remainder Theorem. Let H be a commutative ring with identity, and $G \subseteq H$ a field (whose 0 and unit element are the same as those of H). Let P, P_1, P_2 be monic polynomials in $G[u]$ such that $P = P_1 \cdot P_2$ and $(P_1, P_2) = 1$. Then,

(1) The mapping $m: H[u]/\langle P\rangle \to H[u]/\langle P_1\rangle \times H[u]/\langle P_2\rangle$ given by $m(p) = (m_1(p), m_2(p))$ where $m_i(p) = p \bmod P_i$ $(i = 1, 2)$ is an isomorphism.

(2) The inverse mapping $m^{-1}: H[u]/\langle P_1\rangle \times H[u]/\langle P_2\rangle$ is given by $m^{-1}(p_1, p_2) = (p_1\cdot Q_1 + p_2\cdot Q_2) \bmod P$ where Q_1, Q_2 are polynomials in $G[u]$ such that

$$Q_1 = 1 \bmod P_1 \qquad Q_1 = 0 \bmod P_2$$
$$Q_2 = 0 \bmod P_1 \qquad Q_2 = 1 \bmod P_2$$

(since $(P_1, P_2) = 1$ there exist $A, B \in G[u]$ such that $AP_1 + BP_2 = 1$. We can choose $Q_1 = BP_2$ and $Q_2 = AP_1$).

Remark 10. Since $P_1, P_2 \in G[u]$ the coefficients of $m_1(p)$ and $m_2(p)$ are linear combinations (over G) of the coefficients of p. Since $Q_1, Q_2, P \in G[u]$ the coefficients of $m^{-1}(p_1, p_2)$ are linear combinations (over G) of the coefficients of p_1 and p_2. If we denote the set of coefficients of a polynomial p by $C_{ff}(p)$ we obtain that $L_G(C_{ff}(P)) = L_G(C_{ff}(m_1(p)), C_{ff}(m_2(p)))$.

Remark 11. If $P, P_1, P_2, \ldots, P_k \in G[u]$ are such that $P = \prod_{i=1}^{k} P_i$ and $(P_i, P_j) = 1$ for $i \neq j$ then $m: H[u]/\langle P\rangle \to H[u]/\langle P_1\rangle \times H[u]/\langle P_2\rangle \times \cdots \times H[u]/\langle P_k\rangle$ defined by $m(p) = (m_1(p), \ldots, m_k(p))$ where $m_i(p) = p \bmod P_i$ is an

isomorphism. The inverse mapping m^{-1} is given by $m^{-1}(P_1,..., P_k) = (\sum_{i=1}^{k} p_i Q_i) \bmod P$ where $Q_1,..., Q_k \in G[u]$ satisfy $Q_i = 0 \bmod P_j$ for $j \neq i$ and $Q_i = 1 \bmod P_i$.

Remark 12. If $C_{ff}(p)$ has been computed (or are in $L_G(B)$) then $\{C_{ff}(m_i(p))\}$ can be computed without any m/d steps. Conversely, if $\{C_{ff}(p_i)\}$ has been computed (or are in $L_G(B)$) then $C_{ff}(m^{-1}(p_1,..., p_k))$ can be computed without any m/d steps.

Notation. If $\mathbf{h}$ is a vector whose coordinates are $C_{ff}(p)$ then $m_i(\mathbf{h})$ is the vector whose coordinates are $C_{ff}(m_i(p))$.

LEMMA 12. *Let $P \in G[u]$ be a monic polynomial such that $P = \prod_{i=1}^{s} P_i$, where each P_i is a power of an irreducible polynomial, and the P_i's are pairwise relatively prime. Then $\mu_B(C(P; \mathbf{f}, \mathbf{h})) = \mu_B(\{C(P_i ; \mathbf{f}_i , \mathbf{h}_i)\})$ where $\mathbf{f}_i = m_i(\mathbf{f})$ and $\mathbf{h}_i = m_i(\mathbf{h})$ $(i = 1, 2,..., s)$.*

Proof. Let $\mathscr{A}$ be an algorithm computing $C(P; \mathbf{f}, \mathbf{h})$ using the minimum number of m/d steps. By Remark 12 there exists an algorithm $\mathscr{A}'$ (over $B \cup C(P; \mathbf{f}, \mathbf{h})$) computing $\{C(P_i ; \mathbf{f}_i , \mathbf{h}_i)\}$ using no m/d steps. The algorithm $(\mathscr{A}, \mathscr{A}')$, the concatenation of $\mathscr{A}$ and $\mathscr{A}'$ is an algorithm over B which computes $\{C(P_i ; \mathbf{f}_i , \mathbf{h}_i)\}$ using $\mu_B(C(P; \mathbf{f}, \mathbf{h}))$ m/d steps. This proves the inequality one way. Conversely, let $\mathscr{A}$ be an algorithm computing $\{C(P_i ; \mathbf{f}_i , \mathbf{h}_i)\}$ using the minimum number of m/d steps, then by Remark 12 there exists an algorithm $\mathscr{A}'$ (over $B \cup \{C(P_i ; \mathbf{f}_i , \mathbf{h}_i)\}$) computing $C(P; \mathbf{f}, \mathbf{h})$ using no m/d steps, and $(\mathscr{A}, \mathscr{A}')$ is an algorithm over B computing $C(P; \mathbf{f}, \mathbf{h})$ using $\mu_B(\{C(P_i ; \mathbf{f}_i , \mathbf{h}_i)\})$ m/d steps. This proves the inequality the other way and thus proves the lemma.

THEOREM 2. *Let $G = Q$ the field of rational numbers, $F = Q(w)$ where w is the pth root of unity $(w = e^{2\pi i/p})$, $H = F(y_0 , y_1 ,..., y_{p-1})$. Then $\mu_B(\mathrm{DFT}(p)) = 2p - \psi(p - 1) - 3$, where $\psi(n) = |\{d \mid d \text{ divides } n\}|$.*

Proof. The discussion at the beginning of the section shows that $\mu_B(\mathrm{DFT}(p)) = \mu_B(C(u^{p-1} - 1; \mathbf{w}(i), \mathbf{y}(i))$. Over the field Q of rational numbers $u^{p-1} - 1 = \prod_{d|n} \Phi_d$, where Φ_d is the minimal polynomial whose root is the dth root of unity. By Lemma 12 $\mu_B(\mathrm{DFT}(p)) = \mu_B(\{C(\Phi_d ; \mathbf{f}_d , \mathbf{h}_d) \mid d$ divides $p - 1\}$, where $\mathbf{f}_d = m_d(\mathbf{w}(i))$ and $\mathbf{h}_d = m_d(\mathbf{y}(i))$. By Remark 10, $L_G(\{\mathbf{h}_d\}) = L_G(y_1 ,..., y_{p-1})$ and therefore the substitution which maps the y_j's into the $p - 1$ coordinates of $\{\mathbf{h}_d\}$ is invertible. Let α be the homogeneous substitution such that α^* restricted to the coordinates of $\{\mathbf{h}_d\}$ is a 1:1 mapping into $\{y_1 ,..., y_{p-1}\}$. Let $\mathbf{y}_d = \alpha^*(\mathbf{h}_d)$, then the $\mathbf{y}_d$'s have all distinct coordinates. By Corollary 4, $\mu_B(\{C(\Phi_d ; \mathbf{f}_d , \mathbf{h}_d)\}) = \mu_B(\{C(\Phi_d ; \mathbf{f}_d , \mathbf{y}_d)\})$.

By Remark 10, $L_G(\{\mathbf{f}_d\}) = L_G(\mathbf{w}(i))$. Since the coordinates of $\mathbf{w}(i)$ are $\{w^i \mid i = 1, 2,..., p - 1\}$, we obtain that $\dim L_G(\mathbf{w}(i)) = p - 1$, and that $\{1, w, w^2,..., w^{p-2}\}$ form a basis of $L_G(\{\mathbf{f}_d\})$. Therefore, $rL_G(\{\mathbf{f}_d\}) = L_G(\{r(\mathbf{f}_d)\})$ is of dimension $p - 2$. Since $\Phi_1 = u - 1$, we obtain that $\mathbf{f}_1$ is the one dimen-

sional vector $\sum_{i=1}^{p-1} w(i) = \sum_{i=1}^{p-1} w^i = -1$. By Remark 1, $\mu_B(\mathrm{DFT}(p)) = \mu_B(C(\Phi_d, \mathbf{f}_d, \mathbf{y}_d) \mid d \neq 1\})$ which by Corollary 10 is equal to $2\sum_{d|n, d\neq 1} \deg(\Phi_d) - (\phi(p-1) - 1) = 2(p-2) - \phi(p-1) + 1 = 2p - \phi(p-1) - 3$.

The same method of analysis which yielded Theorem 2 can be used to determine the multiplicative complexity of DFT(p) when G is taken to be a field other than that of rational numbers. We will illustrate this by an example.

EXAMPLE 1. Let w be the 7th root of unity and let $a = w + w^6$. Let $G = Q(a)$, $F = G(w)$ and $H = F(y_0, y_1, \ldots, y_6)$. We want to determine $\mu_B(\mathrm{DFT}(7))$ where $B = F \cup \{y_0, \ldots, y_6\}$. That is, we want to compute $\overline{Y}_i = \sum_{j=0}^{6} w^{ij} y_j$, $(i = 0, 1, \ldots, 6)$. Since $\overline{Y}_0 = \sum_{j=0}^{6} y_j$ it can be computed without any m/d step. For $i = 1, 2, \ldots, 6$, $\overline{Y}_i = y_0 + \sum_{j=1}^{6} w^{ij} y_j = y_0 + Y_i$, so computing the Y_i's and $\overline{Y}_i$'s require the same number of m/d steps.

Using the permutation $\prod$ and the mapping t described in the beginning of the section we see that

$$\begin{pmatrix} Y_1 \\ Y_3 \\ Y_2 \\ Y_6 \\ Y_4 \\ Y_5 \end{pmatrix} = \begin{pmatrix} w^1 & w^5 & w^4 & w^6 & w^2 & w^3 \\ w^3 & w^1 & w^5 & w^4 & w^6 & w^2 \\ w^2 & w^3 & w^1 & w^5 & w^4 & w^6 \\ w^6 & w^2 & w^3 & w^1 & w^5 & w^4 \\ w^4 & w^6 & w^2 & w^3 & w^1 & w^5 \\ w^5 & w^4 & w^6 & w^2 & w^3 & w^1 \end{pmatrix} \begin{pmatrix} y_1 \\ y_5 \\ y_4 \\ y_6 \\ y_2 \\ y_3 \end{pmatrix},$$

that is, $Y_1 + Y_2 u + Y_3 u^2 + y_6 u^3 + y_4 u^4 + y_5 u^5 = R(u) \cdot S(u) \bmod u^6 - 1$ where $R(u) = w^1 + w^3 u + w^2 u^2 + w^6 u^3 + w^4 u^4 + w^5 u^5$ and $S(u) = y_1 + y_5 u + y_4 u^2 + y_6 u^3 + y_2 u^4 + y_3 u^5$. Since $u^6 - 1 = (u-1)(u+1)(u^2+u+1)(u^2-u+1)$ and all the factors are irreducible (over $G = Q(a)$) we obtain by Lemma 12 that computing DFT(7) has the same multiplicative complexity as that of computing the coefficients of the polynomial T_1, T_2, T_3, and T_4 where

$$T_1 = R(u) \cdot S(u) \bmod u - 1 = \left(\sum_{i=1}^{6} w_i\right)\left(\sum_{i=1}^{6} y_i\right) = -\sum_{i=1}^{6} y_i$$

$$\begin{aligned} T_2 &= R(u) \cdot S(u) \bmod u + 1 \\ &= (w + w^2 - w^3 + w^4 - w^5 - w^6)(y_1 + y_2 + y_3 + y_4 + y_5 + y_6) \end{aligned}$$

$$\begin{aligned} T_3 &= R(u) \cdot S(u) \bmod u^2 + u + 1 \\ &= ((w + w^6 - w^2 - w^5) + (w^3 + w^4 - w^2 - w^5)\, u) \\ &\quad \times (y_1 + y_6 - y_3 - y_4) + (y_2 + y_5 - y_3 - y_4)\, u) \bmod u^2 + u + 1 \end{aligned}$$

$$\begin{aligned} T_4 &= R(u) \cdot S(u) \bmod u^2 - u + 1 \\ &= ((w - w^2 + w^5 - w^6) + (w^2 + w^3 - w^4 - w^5)\, u) \\ &\quad \times ((y_1 + y_3 - y_4 - y_6) + (-y_2 - y_3 + y_4 + y_5)\, u) \bmod u^2 - u + 1 \end{aligned}$$

Since $a = w + w^6$ then $a^2 = w^2 + w^5 + 2$ and $a^3 = w^3 + w^4 + 3a$. So

$w^2 + w^5 \in G$ and $w^3 + w^4 \in G$. Consequently, the coefficients of T_2 (as well as of T_1) are in $L_G(B)$. Since $1 + w + w^2 + w^3 + w^4 + w^5 + w^6 = 0$ we obtain that $a^3 + a^2 - 2a - 1 = 0$. But $u^3 + u^2 - 2a - 1$ is irreducible over Q, so $G = Q(a)$ is a cubic extension of Q. Since $G(w) = Q(w)$ which has dimension 6 (over Q) we see that $G(w)$ is a quadratic extension of G. The set $\{1, a, a^2\}$ form a basis of G (over Q) so none of the elements $b = ((w - w^6) + (w^2 - w^5) - (w^3 - w^4)$, $c = ((w - w^6) - (w^2 - w^5))$, and $d = ((w^2 - w^5) + (w^3 - w^4))$ are in G. Let $\{1, d\}$ be a basis of $G(w)$ over G, then there exist $g_1, g_2, g_3, g_4 \in G$ ($g_1, g_3 \neq 0$ such that $b = g_1 d + g_2$, $c = g_3 \cdot d + g_4$. Applying Theorem 1 to the computation of $C_{ff}(T_1) \cup C_{ff}(T_2)$, and taking $J = \{1\}$ we obtain $\mu_B(\mathrm{DFT}(7)) = \mu_B(C_{ff}(T_1), C_{ff}(T_2)) \geqslant \deg(u+1) + (\deg(u^2 - u + 1) - 1) + \dim L_G(r(c), r(d)) = 3$. To show that the inequality can be replaced by equality we will give an algorithm for computing $C_{ff}(T_1 \cup C_{ff}(T_2)$ using 3 m/d steps.

Let

$$m_1 = b \cdot (y_1 + y_2 - y_3 + y_4 - y_5 - y_6),$$
$$m_2 = c \cdot (y_1 + y_3 - y_4 - y_6),$$
$$m_3 = d \cdot (-y_2 - y_3 + y_4 + y_5).$$

Then the coefficient of T_1 is m_1, the constant coefficient of T_2 is $m_2 - m_3$, and the linear coefficient of T_2 is $g^{-1}(m_2 - h) + g_3 m_3$ where $h = g_4((y_1 + y_3 - y_4 - y_6) - g_3(y_2 - y_3 + y_4 + y_5))$ $L_G(B)$. It is clear how to construct an algorithm using 3 m/d steps to compute $C_{ff}(T_1) \cup C_{ff}(T_2)$ using these identities.

We will next derive a lower bound of the multiplicative complexity of DFT(n) where $n = p^k$ is a power of a prime number $p \neq 2$, and $B = Q(w) \cup \{y_0, \ldots, y_{n-1}\}$, where w is the nth root of unity. As before, we define $Y_i = \sum_{j=1}^{n-1} w^{ij} y_j$. We will derive a lower bound of the multiplicative complexity of $\{Y_i \mid (i, p) = 1\}$. Since $\mu_B(\mathrm{DFT}(p^k)) = \mu_B(\{Y_i \mid i = 1, \ldots, p^k - 1)) \geqslant \mu_B(\{Y_i \mid (i, p) = 1\})$, this lower bound is also a lower bound of $\mu_B(\mathrm{DFT}(p^k))$.

Let $\alpha: \{y_1, \ldots, y_{n-1}\} \to L_Q(B)$ be defined by $\alpha(y_i) = y_i$ if $(i, p) = 1$ and $\alpha(y_i) = 0$ if $(i, p) \neq 1$. Define $z_i = \alpha^*(Y_i) = \sum_{(j,p)=1} w^{ij} y_j$ for all $i = 1, 2, \ldots, p^k - 1$ such that $(i, p) = 1$. By Lemma 8 and Lemma 4, $\mu_B(\{Y_i \mid (i, p) = 1\} \geqslant \mu_B(\{z_i\})$. Let M_n be the group of integers smaller than $n = p^k$ which are relatively prime to p, with group operation multiplication modulo p^k. We will denote the elements of M_n by $\{m_i \mid (i, p) = 1\}$ such that $m_i \cdot m_j = m_r$ if and only if $i \cdot j = r \bmod p^k$.

The same calculation as at the beginning of the section show that

$$\sum_{(i,p)=1} z_i m_i = \Big(\sum_{(i,p)=1} w^i m_i \Big) \Big(\sum_{(i,p)=1} y_i (m_i)^{-1} \Big),$$

and defining a permutation π by $\pi(i) = j$ if $m^{-1} = m_j$ we again obtain that

$$\sum_{(i,p)=1} z_i m_i = \Big(\sum_{(i,p)=1} w^i m_i \Big) \Big(\sum_{(i,p)=1} y_{\pi(i)}, m_i \Big).$$

The group M_n is isomorphic to the cyclic group of $p^{k-1}(p-1)$ elements. (It is this isomorphism which is false when $p=2$. The group M_n for $n=2^k$ $(k>1)$ is isomorphic to $z_2 \times z_m$ where $m=2^{k-2}$. We will therefore treat the case that $n=2^k$ separately.) Let $t: M_n \to z_s$ $(s=p^{k-1}\cdot(p-1))$ be an isomorphism between M_n and the cyclic group $\{1, u, u^2,..., u^{s-1}\}$ of $s=p^{k-1}(p-1)$ elements. As just before Theorem 2 we denote by $y(i)$ the indeterminate y_j such that $t^{-1}(u^i)=m_k$ and $j=\pi(k)$; we denote by $w(i)$ the element w^j such that $m_j=t^{-1}(u^i)$; and by $z(i)$ the element z_j such that $m_j=t^{-1}(u^i)$. Using this notation we obtain, as before, that

$$\sum_{i=0}^{s-1} z(i)\,u^i = \left(\sum_{i=0}^{s-1} w(i)\,u^i\right)\left(\sum_{i=0}^{s-1} y(i)\,u^i\right) \bmod u^s - 1.$$

Remark 13. Let $I_0=\{i \mid i=ap^{k-2}(p-1),\ a=0,1,...,p-1\}$ and $J_0=\{j \mid j=bp^{k-1}+1,\ b=0,1,...,p-1\}$. For each $j\in J_0$, $(m_j)^p=m_1$ and therefore $t(m_j)=u^i$ for some $i\in I_0$. Since t is one-one we obtain that $t\{m_j \mid j\in J_0\}=\{u^i \mid i\in I_0\}$, therefore $\{w(i) \mid i\in I_0\}=\{w^j \mid j\in J_0\}$. For each $l=1,2,...,p^{k-2}(p-1)-1$ we define $I_l=\{i+l \mid i\in I_0\}$ and $J_l=\{j\cdot r \bmod p^k \mid j\in J_0,\ t(m_r)=u^l\}$. For each $i\in I_l$, $u^i=u^{i'}\cdot u^l$ for some $i'\in I_0$, and therefore $t^{-1}(u^i)=m_j\cdot m_r=m_j$ where $j'\in J_0$ and $j=j'\cdot r \bmod p^k$, so $j\in J_l$. Therefore $\{w(i) \mid i\in I_l\}=\{w^j \mid j\in J_l\}$. Since the I_l's $(l=0,1,...,p^{k-2}(p-1)-1)$ form a partition of $\{0,1,...,s-1\}$, the J_l's form a partition of $\{j \mid j<p^k,(j,p)-1\}$.

Remark 14. Clearly, $(bp^{k-1}+1)\cdot r \bmod p^k = b'\cdot p^{k-1}+r'$ where $r'<p^{k-1}$ is given by $r=c\cdot p^{k-1}+r'$, and $b'<p$ is given by $b'=b\cdot r+c \bmod p$. Therefore, for every l there exists an $r'=r'(l)$ such that $J_l=\{j \mid j=bp^{k-1}+r'(l),\ b=0,1,...,p-1\}$.

Remark 15. Let $m=p^{k-1}$, then w^m is the pth root of unity, and therefore $\sum_{b=0}^{p-1} w^{mb}=0$. By Remarks 13 and 14, $\sum_{i\in J_l} w(i)=\sum_{j\in J_l} w^j = w^{r'}(\sum_{i=0}^{p-1} w^{bm})=0$.

Remark 16. As before, we denote p^{k-1} by m, $p^{k-1}(p-1)$ by s and p^k by n. The polynomial $\Phi_n=\sum_{i=0}^{p-1} u^{mi}$ is the minimal degree polynomial having w as the root. Therefore, $\{1, w, w^2,..., w^{s-1}\}$ form a basis of $Q(w)$ (over Q). Denoting, as before, by ρ the natural vector space homorphism $\rho: Q(w)\to Q(w)/Q$, we see that $\{\rho(w), \rho(w^2),..., \rho(w^{s-1})\}$ form a basis of $\rho(Q)$. Therefore $\{\rho(w^i) \mid i<s,\ (i,p)=1\}$ form a linearly independent set. Since each J_l has exactly one element greater than s (namely, $(p-1)p^{k-1}+r'(l)$), $\sum_{j\in J_l} w^j=0$ we see that the dimension of $L_Q(\{w^j \mid (j,p)=1, j<p^k\})$ is the same as the cardinality of $\{j \mid j<s,(j,p)=1\}$, namely, $(p-1)^2p^{k-2}$.

LEMMA 13. *Let* $R(u)=\sum_{i=0}^{s-1} w(i)\,u^i$ $(s=p^{k-1}(p-1), k>1)$, *let* $R_1(u)=R(u) \bmod u^r-1$ $(r=p^{k-2}(p-1))$, *and let* $R_2(u)=R(u) \bmod \sum_{i=0}^{p-1}(u^r)^i=\sum_{i=0}^{q-1} f_i u^i q=(p-1)^2p^{k-2}$. *Then*:

(1) $R_1(u) = 0$

(2) $\dim L_Q(\{\rho(f_i)\}) = q$.

Proof. Setting $u^r = 1$ in $R(u)$ we see that each coefficient of $R_1(u)$ is $\sum_{i \in I_l} w(i)$ for some l. which by Remark 15 is 0. By Remark 10 $L_Q(\{w(i)\}) = L_Q(C_{ff}(R(u))) = L_Q(C_{ff}(R_1(u),\ C_{ff}(R_2(u)))) = L_Q(C_{ff}(R_2(u))) = L_Q(\{f_i\})$. So $L_Q(\{\rho(w(i))\}) = L_Q(\{\rho(f_i)\})$. By Remark 16, $\dim L_Q(\{\rho(w(i))\}) = (p-1)^2 p^{k-2} = q$.

THEOREM 3. *Let $p \neq 2$ be a prime number, then for any $k \geqslant 2$, $\mu_B(\mathrm{DFT}(p^k)) \geqslant 2(p-1)^2 p^{k-2} - \phi(p-1)$, where $B = Q(w) \cup \{y_0, \ldots, y_{n-1}\}$ $(n = p^k)$, $G = Q$, and $\phi(p-1) =$ no. of divisors of $p-1$.*

Proof. Let $R(u) = \sum_{i=0}^{l-1} w(i)\, u^i$ $(s = p^{k-1}(p-1))$, $S(u) = \sum_{i=0}^{s-1} y(i)\, u^i$, and $T(u) = R(u) \cdot S(u) \bmod u^s - 1$. Let $T_1(u) = T(u) \bmod u^r - 1$ $(r = p^{k-2}(p-1))$, $T_2(u) = T(u) \bmod \sum_{i=0}^{p-1} (u^r)^i$. The discussion prior to Remark 13 showed that $\mu_B(\mathrm{DFT}(p^k)) \geqslant \mu_B(\{z(i)\}) = \mu_B(C_{ff}(T(u))) = \mu_B(C_{ff}(T_1(u)),\ C_{ff}(T_2(u))) = \mu_B(C_{ff}(T_2(u)))$. (The last two equalities are by Lemmas 12 and 13, respectively.) By Lemma 12, $\dim L_Q(\rho(C_{ff}(R_2(u))) = q = \deg(\sum_{i=0}^{p-1} (u^r)^i)$ and therefore, using the same argument as in the proof of Theorem 2 (using Lemmas 8 and 12, and Corollary 10) we see that $\mu_B(C_{ff}(T_2(u)) = \deg(\sum_{i=0}^{p-1} (u^r)^i) + \dim L_Q(\rho(C_{ff}(R_2(u))) - d$ where d is the number of irreducible polynomials dividing $\sum_{i=0}^{p-1} (u^r)^i$. So $\mu_B(\mathrm{DFT}(p^k)) \geqslant 2q - d = 2(p-2)^2 p^{k-2} - d$.

To finish the proof we have to calculate d. The polynomial $u^s - 1$ has $\phi(s) = k\phi(p-1)\,\phi(p-1)$ irreducible factors, and since $(u^r - 1)(\sum_{i=0}^{p-1} (u^r)^i) = u^s - 1$, we see that the number d of irreducible factors of $\sum_{i=0}^{p-1} (u^r)^i$ is $k\phi(k-1) - (k-1)\,\phi(k-1) = \phi(k-1)$. This proves the theorem.

As was mentioned before, the group $M_n (n = 2^k)$ of odd numbers smaller than n with group operation multiplication modulo n, is not cyclic. We will show the well known fact that M_n is isomorphic to $z_2 \times z_m (m = 2^{k-2})$ for $k \geqslant 3$, by exhibiting an isomorphism, which we will need to estimate the multiplicative complexity of $\mathrm{DFT}(2^k)$.

LEMMA 14. *For each $k \geqslant 3$, $5^{2^{k-3}} = 2^{k-1} + 1 \bmod 2^k$.*

Proof. We will prove the lemma by induction on k. For $k = 3$ the result is obvious. Assume the result proved for k, then $5^{2^{k-3}} = 2^{k-1} + 1 + a \cdot 2^k \bmod 2^{k+1}$ $(a \in \{0, 1\})$. Squaring both sides, we obtain

$$\begin{aligned} 5^{2^{k-2}} &= 2^{2^{k-2}} + 1 + a^2 2^{2^k} + 2^k + a 2^{2^k} + a 2^{k+1} \bmod 2^{k+1} \\ &= 2^k + 1 \bmod 2^{k+1}. \end{aligned}$$

We will denote the elements of M_n $(n = 2^k)$ by $\{m_i \mid i = 2s + 1,\ s = 0, 1, \ldots, 2^{k-1} - 1\}$ with multiplication given by $m_i \cdot m_j = m_l$ if $i \cdot j = l \bmod 2^k$. We will

denote the elements of $z_2 \times z_{2^{k-2}}$ by $\{v^i u^j \mid i = 0, 1,\ j = 0, 1, \ldots, 2^{k-2} - 1\}$, where $u \cdot v = vu$, $v^2 = 1$, $u^{2^{k-2}} = 1$.

LEMMA 15. *M_n ($n = 2^k$, $k \geqslant 2$) is isomorphic to $z_2 \times z_{2^{k-2}}$. The isomorphism is given by $t(m_5) = u$, $t(m_{n-1}) = v$. (For $k = 2$ we replace m_5 by m_1).*

Proof. A direct computation verifies the assertion for $k = 2$. Assume $k \geqslant 3$. Since $(m_{n-1})^2 = m_1$, and $(m_s)^2 = 1$ ($s = 2^{k-1} + 1$) we see that M_n is not cyclic, because the cyclic group $\{u^i \mid i = 0, 1, \ldots, 2^{k-1} - 1, u^{2^{k-1}} = 1\}$ of order 2^{k-1} has only one element $u^j \neq 1$ such that $(u^j)^2 = 1$. Therefore M_n is isomorphic to the direct product of cyclic groups of orders of powers of 2, such that the product of the orders is 2^{k-1}. By Lemma 14, the order of m_5 is 2^{k-2}, and therefore M_n is isomorphic to $z_2 \times z_{2^{k-2}}$. Since $(m_{n-1})^2 = m_1$, and $n - 1 \neq 2^{k-3} + 1$, m_{n-1} is not in the subgroup generated by m_5. Therefore $gp(m_5) \cap gp(m_{n-1}) = \{m_1\}$, and since $|gp(m_5)| \times |gp(m_{n-1})| = 2^{k-2} \cdot 2 = 2^{k-1} = |M_n|$, we see that $M_n = gp(m_5, m_{n-1})$. This proves the lemma.

Let $z_i = \sum_{(j,2)=1} w^{ij} y_j$, $i = 1, 3, 5, \ldots, 2^k - 1$, w the nth root of unity, $n = 2^k$. Just as in the discussion preceding Theorems 2 and 3 we obtain $\sum_{(i,2)=1} z_i m_i = (\sum_{(i,2)=1} w^i m_i)(\sum_{(i,2)=1} y_{\pi(i)} m_i)$ where $\pi(i) = j$ *if* $m_i = (m_j)^{-1}$. Let t be the isomorphism of Lemma 15, we denote by $y(i, j)$ the indeterminate y_l such that $t^{-1}(u^i v^j) = (m_l)^{-1}$; we denote by $w(i, j)$ the element wl such that $t^{-1}(u^i v^j) = m_l$; and by $z(i, j)$ the element z_l such that $t^{-1}(u^i v^j) = m_l$. Therefore the $z(i, j)$'s can be expressed as the coefficients of the polynomial

$$\sum_{i=0}^{s-1} \sum_{j=0}^{1} z(i, j)\, u^i v^j = \left(\sum_{i=0}^{s-1} \sum_{j=0}^{1} w(i, j)\, u^i v^j\right)\left(\sum_{i=0}^{s-1} \sum_{j=0}^{1} y(i, j)\, u^i v^j\right) \bmod (u^s - 1, v^2 - 1),$$

where $s = 2^{k-2}$.

Remark 17. Let G and H be as in the statement of the Chinese Remainder Theorem. Let $P \in G[u]$, $Q, Q_1, Q_2 \in G[v]$ such that $Q = Q_1 \cdot Q_2$ and $(Q_1, Q_2) = 1$. Then $H[u, v]/\langle P(u), Q(v)\rangle$ is isomorphic to $H'[v]/\langle Q(v)\rangle$, where $H' = H[u]/\langle P(u)\rangle$. By the Chinese Remainder Theorem $H'[v]/\langle Q(v)\rangle$ is isomorphic to $H'[v]/\langle Q_1(v)\rangle \times H'[v]/\langle Q_2(v)\rangle$. Therefore, $H[u, v]/\langle P(u), Q(v)\rangle$ is isomorphic to $H[u, v]/\langle P(u), Q_1(v)\rangle \times H[u, v]/\langle P(u), Q_2(v)\rangle$.

Remark 18. Let G, H, P, Q be as in Remark 17, and let $P(u) = \prod_i P_i(u)$ ($P_i(u) \in G[u]$), $Q(v) = \prod_j Q_j(v)$ ($Q_j(v) \in G[v]$) such that $(P_r, P_s) = 1$ for $r \neq s$ and $(Q_r, Q_s) = 1$ for $r \neq s$. Then $H[u, v]/\langle P(u), Q(v)\rangle$ is isomorphic to $\prod_{(i,j)} H[u, v]/\langle P_i(u), Q_j(v)\rangle$. Moreover, let m be the isomorphism and for every $p(u, v) \in H[u, v]/\langle P(u), Q(v)\rangle$ let $m(p) = (p_{i,j}(u, v))$ then $L_G(C_{ij}(p(u, v)) = L_G(\{C_{ij}(p_{i,j}(u, v))\})$.

LEMMA 16. *Let $s = 2^{k-2}$ and $r = 2^{k-3}$ ($k \geqslant 3$). There exist $\mathbf{f}_1, \mathbf{f}_2 \in Q(w)^r$, $\mathbf{h}_1, \mathbf{h}_2 \in L_Q(y(i, j))^r$ such that:*

(1) $L_Q(\mathbf{h}_1, \mathbf{h}_2) = L_Q(\{y(i,j) - y(i+r,j) \mid 0 \leqslant i < r, 0 \leqslant j < 2\}$. *That is the* $s = 2r$ *coordinates of* $\mathbf{h}_1$ *and* $\mathbf{h}_2$ *are invertible linear coordinations (over* Q*) of the set* $\{y(i,j) - y(i+r,j) \mid 0 \leqslant i < r, 0 \leqslant j < 2\}$.

(2) $L_Q(\mathbf{f}_1, \mathbf{f}_2) = L_Q(w, w^3, w^5, \ldots, w^{2s-1})$.

(3) $L_Q(\{z(i,j) \mid 0 \leqslant i < s, 0 \leqslant j < 2\}) = L_Q(C(u^r + 1; \mathbf{f}_1, \mathbf{h}_1), C(u^r + 1; \mathbf{f}_2, \mathbf{h}_2))$.

Proof. $R(u,v) = \sum_{i=0}^{s-1} \sum_{j=0}^{1} w(i,j) u^i v^j$, $S(u,v) = \sum_{i=0}^{s-1} \sum_{j=0}^{1} y(i,j) u^i v^j$, and $T(u,v) = \sum_{i=0}^{s-1} \sum_{j=0}^{1} z(i,j) u^i v^j = R(u,v) \cdot S(u,v) \mod (u^s - 1, v^2 - 1)$. Since $u^s - 1 = (u^r - 1)(u^r + 1)$, $v^2 - 1 = (v-1)(v+1)$ we define for $a \in \{-1, 1\}$, $b \in \{-1, 1\}$, $R_{a,b}(u,v) = R(u,v) \mod (u^r + a, v + b)$, $S_{a,b}(u,v) = S(u,v) \mod (u^r + a, v + b)$ and $T_{a,b}(u,v) = T(u,v) \mod (u^r + a, v + b)$. By Remark 18 we obtain $L_Q(\{C_{ff}(R_{a,b})\}) = L_Q(C_{ff}(R))$; $L_Q(\{C_{ff}(S_{a,b})\}) = L_Q(C_{ff}(S))$; and $L_Q(\{C_{ff}(T_{a,b})\}) = L_Q(C_{ff}(T)) = L_Q(\{z(i,j)\})$. By Lemma 14 and the definition of t, $t^{-1}(u^r) = m_{2s+1}$. Since $n = 2^k = 4s$ we obtain that $w^{2s} = -1$. Therefore if $t^{-1}(u^i v^j) = m_i$ we have $t^{-1}(u^{i+r} v^j) = t^{-1}(u^r)\, t^{-1}(u^i v^j) = m_{2s+1} \cdot m_i = m_x$, where $x = (2s+1) \cdot l \bmod 2^k = 2sl + l \bmod 2^k = 2s + l \bmod 2^k$ (recall that by definition, l is odd and $4s = 2^k$). Consequently, $w(i+r,j) = w^q = w^{2s+l} = w^{2s} w^l = -w^l = -w(i,j)$. Since the $u^i v^j$ coefficient of $R(u,v) \bmod u^r - 1$ $(i = 0, 1, \ldots, r-1; j = 0, 1)$ is $w(i,j) + w(i+r,j)$, we see that $R(u,v) \bmod u^r - 1 = 0$ and therefore $T(u,v) \bmod u^r - 1 = 0$ which implies that $T_{-1,b} = 0$ for $b \in \{-1, 1\}$. Consequently, $L_Q(\{z(i,j)\}) = L_Q(C_{ff}(T_{1,1}), C_{ff}(T_{1,-1}))$.

The set of coefficients of $R(u,v) \bmod u^r + 1$ is $\{2w, 2w^3, 2w^5, \ldots, 2w^{2s-1}\}$, and the set of coefficients of $S(u,v) \bmod u^r + 1$ is $\{y(i,j) - y(i+r,j) \mid 0 \leqslant i < r, 0 \leqslant j < 2\}$. Let $\mathbf{f}_1$ be the vector of coefficients of $R_{1,-1}$, and $\mathbf{f}_2$ the vector of coefficients of $R_{1,1}$. Let $\mathbf{h}_1$ be the vector of coefficients of $S_{1,-1}$, and $\mathbf{h}_2$ the vector of coefficients of $S_{1,1}$. The lemma follows from Remark 18 and the observation that the $R_{1,b}$'s, $S_{1,b}$'s, and $T_{1,b}$'s are constants as polynomials of v, that is, they depend only on u, and therefore $T_{1,b} = R_{1,b} \cdot S_{1,b} \bmod u^r + 1$.

Remark 19. The minimal polynomial of w is $u^{2s} + 1$. Therefore $\{1, w, w^2, \ldots, w^{2s-1}\}$ are linearly independent (over Q). Denoting by ρ the vector space homomorphism $\rho: Q(w) \to Q(w)/Q$ we obtain that $\{\rho(w), \rho(w^2), \ldots, \rho(w^{2s-1})\}$ are linearly independent. Consequently, $\{\rho(\mathbf{f}_1), \rho(\mathbf{f}_2)\}$ the images under ρ of the coordinates of $\mathbf{f}_1$ and $\mathbf{f}_2$ form a linearly independent set.

The reason that the polynomial $T_{-1,b}$ was 0 in the proof of Lemma 16, was that $w^{2s+i} = -w^i$, that is $Z_i = \sum_{(j,2)=1} w^{ij} y_j = \sum_{j=0}^{s-1} w^{i(2j+1)} (y_{2j+1} - y_{2j+1+2s})$, $(i = 1, 3, \ldots, 2^k - 1)$. (For the same reason we also obtain $z_{i+2s} = -z_i$ for $i = 1, 3, \ldots, 2s-1$). Motivated by this observation, we define for every $\mathbf{h} \in L_Q(\{y_j\})^s$, $U_i = \sum_{j=0}^{s-1} w^{i(2j+1)} h_j$ $(i = 1, 3, \ldots, 2^k - 1)$. We denote the set $\{U_i \mid i = 1, 3, \ldots, 2^k - 1\}$ by $U(2^k, \mathbf{h})$.

COROLLARY 11. *Let* s *and* r *be as in Lemma* 16. *For each* $\mathbf{h} \in L_Q(\{y_j\})^s$, *there exist* $\mathbf{f}_1, \mathbf{f}_2 \in Q(w)^r$, $\mathbf{h}_1, \mathbf{h}_2 \in L_Q(\{y_j\})^r$ *such that*

(1) $L_Q(\mathbf{h}_1, \mathbf{h}_2) = L_Q(\mathbf{h})$

(2) $L_Q(\mathbf{f}_1, \mathbf{f}_2) = L_Q(w, w^3, \ldots, w^{2^{s-1}})$

(3) $L_Q(U(2^k, \mathbf{h})) = L_Q(C(u^r + 1; \mathbf{f}_1, \mathbf{h}_1), C(u^r + 1; \mathbf{f}, \mathbf{h}_2))$.

LEMMA 17. *For each* $k \geqslant 3$ *there exists a substitution* α *such that* $\alpha^*(\mathrm{DFT}(2^k)) = \{\mathrm{DFT}(2^{k-1}), U(2^k, \mathbf{h})\}$, *where* $h_i = y_{2s+2i+1}$ $(i = 0, 1, \ldots, 2 - 1)$.

Proof. Let $\mathrm{DFT}(2^k)$ be $Y_i = \sum_{j=0}^{n-1} w^{ij} y_j$ $(n = 2^k)$. For $i = 2l$ we have $w^{i(j+2s)} = w^{ij+4ls} = w^{ij}$ (recall that $4s = 2^k$). So, $Y_{2l} = \sum_{j=0}^{2s-1} (w^2)^{lj} (y_j + y_{j+2s})$ $(l = 0, 1, \ldots, 2s - 1)$. For $i = 2l + 1$ we have $w^{i(j+2s)} = w^{ij+2s+4ls} = w^{2s} w^{ij}$. So for $i = 2l + 1$, $Y_{2l+1} = \sum_{j=0}^{s-1} w^{(2l+1)j} (y_j - y_{j+2s})$ $(l = 0, 1, \ldots, 2s - 1)$. Define α by:

$$\begin{aligned}
\alpha(y_j) &= \tfrac{1}{2} y_j && \text{for } j = 2l && l = 0, 1, \ldots, s - 1 \\
\alpha(y_{j+2s}) &= \tfrac{1}{2} y_j && \text{for } j = 2l && l = 0, 1, \ldots, s - 1 \\
\alpha(y_j) &= \tfrac{1}{2}(y_j + y_{j+2s}) && \text{for } j = 2l + 1 && l = 0, 1, \ldots, 2 - 1 \\
\alpha(y_{j+2s}) &= \tfrac{1}{2}(y_j - y_{j+2s}) && \text{for } j = 2l + 1 && l = 0, 1, \ldots, s - 1.
\end{aligned}$$

Using this α we obtain $\alpha^*(y_j + y_{j+2s}) = y_j$ for $j = 0, 1, \ldots, 2s - 1$; $\alpha^*(y_j - y_{j+s}) = 0$ for $j = 2l$, $l = 0, 1, \ldots, s - 1$; and $\alpha^*(y_j - y_{j+2s}) = y_{j+2s}$ for $j = 2l + 1$, $l = 0, 1, \ldots, s - 1$. Therefore $\alpha^*(\{y_{2l}\}) = \mathrm{DFT}(2^{k-1})$ and $\alpha^*(\{Y_{2l+1}\}) = U(2^k, \mathbf{h})$ where $h_i = 2s + 2i + 1$ $(i = 0, 1, \ldots, s - 1)$.

Repeated application of Lemma 17 yields:

COROLLARY 12. *For every* $k \geqslant 3$ *there exists a substitution* α *such that* $\alpha^*(\mathrm{DFT}(2^k)) = \{U(2^k, \mathbf{h}_k), U(2^{k-1}, \mathbf{h}_{k-1}), \ldots, U(2^3, \mathbf{h}_3), \mathrm{DFT}(4)\}$, *and such that all the coordinates of the* $\mathbf{h}_k$*'s as well as* y_0, y_1, y_2, y_3 (*which appear in* $\mathrm{DFT}(4)$) *are linearly independent. Therefore* $\dim L_Q(\{\mathbf{h}_k\} \cup \{y_0, y_1, y_2, y_3\}) = 2^{k-1} + 2$.

Remark 20. Let $B = Q(w) \cup \{y_0, \ldots, y_{n-1}\}$ $(= 2^k)$. $G = Q$, since $\dim L_Q(r(\mathrm{DFT}(4)) = 1$ (r defined before Remark 2) we have $\mu_B(\mathrm{DFT}(4)) \geqslant 1$. In fact it is easy to construct an algorithm (over B) using only one m/d step. Therefore, $\mu_B(\mathrm{DFT}(4)) = 1$.

THEOREM 4. *Let* $B = Q(w) \cup \{y_0, \ldots, y_{n-1}\}$ $(n = 2^k, \ w^n = 1, \ k \geqslant 3)$, $G = Q$, *then* $\mu_B(\mathrm{DFT}(2^k)) \geqslant 2^k - 2k + 1$.

Proof. By Corollary 12 there exists a substitution α such that $\alpha^*(\mathrm{DFT}(2^k)) = \{U(2^k, \mathbf{h}_k), \ldots, U(2^3, \mathbf{h}_3), \mathrm{DFT}(4)\}$. Let β be the substitution $\beta(y_i) = 0$ for $i = 0, 1, 2, 3$; and $\beta(y_i) = y_i$ for $i \geqslant 4$. By Lemmas 4, 5 (and Lemma 8) we have

$$\begin{aligned}
\mu_B(\mathrm{DFT}(2^k)) &\geqslant \mu_B(\alpha^* \mathrm{DFT}(2^k)) = \mu_B(\{U(2^l, \mathbf{h}_l) \mid l = 3, 4, \ldots, k\} \cup \mathrm{DFT}(4)) \\
&\geqslant \mu_B(\{\beta^* U(2^l, \mathbf{h}_l) \mid l = 3, \ldots, k\} \cup \beta^* \mathrm{DFT}(4)) + 1 \\
&= \mu_B(\{U(2^l, \mathbf{h}_l) \mid l = 3, \ldots, k\}) + 1.
\end{aligned}$$

By Corollary 11 we can replace $U(w^{l+3}, \mathbf{h}_{l+3})$ $(l = 0, 1,..., k-3)$ by

$$C(u^{2^l}+1; \mathbf{f}_{l,1}, \mathbf{h}_{l,1}) \cup C(u^{2^l}+1; \mathbf{f}_{l,2}, \mathbf{h}_{l,2})$$

such that

$$L_Q(\mathbf{f}_{l,1}, \mathbf{f}_{l,2}) = L_Q(w^{d(l)}, (w^{d(l)})^3, (w^{d(l)})^5,..., (w^{d(l)})^{m(l)-1})$$

where $d(l) = 2^{k-l-3}$ and $m(l) = 2^{l+2}$; and all the coordinates of the $\mathbf{h}_{l,i}$'s are linearly independent. For every $0 < j < 2^{k-1}$ we have $j = 2^m(2i+1)$, and if $m < k-2$ then choosing $l = k-m-3 \geqslant 0$, $m = k-l-3$. Therefore $w^j = (w^{d(l)})^{2i+1}$ for some i such that $2i+1 \leqslant m(l)-1$. Consequently, $w^j \in L_Q(\mathbf{f}_{l,1}, \mathbf{f}_{l,2})$. Therefore $L_Q(\{\mathbf{f}_{l,1}, \mathbf{f}_{l,2} \mid l = 0, 1,..., k-3\}) = L_Q(\{w^j \mid 0 < j < 2^{k-1}, j \neq 2^{k-2}\}$ and by Remark 19 $\dim L_Q(\rho(\{\mathbf{f}_{l,1}, \mathbf{f}_{l,2} \mid l = 0, 1,..., k-3\})) = 2^{k-1} - 2$. Since

$$\sum_{rl=0}^{k-3} \dim(U^{2^l}+1) = (2^{k-2}-1)$$

we obtain by 10 that

$$\begin{aligned}\mu_B(\{u(2^l, \mathbf{h}_l) \mid l = 3, 4,..., k\}) &= \mu_B(\{C(u^{2^l}+1, \mathbf{f}_{il,1}, \mathbf{h}_{l,1}) \\ &\quad \cup C(u^{2^l}+1; \mathbf{f}_{l,2}, \mathbf{h}_{l,2} \mid l = 0, 1,..., k-3\}) \\ &= 2(2^{k-1}-2) - 2(k-2) = 2^k - 2k.\end{aligned}$$

Therefore, $\mu_B(\mathrm{DFT}(2^k)) \geqslant 2^k - 2k + 1$.

We now turn our attention to computing the DFT(n) where n has at least two distinct prime divisors. All the ideas of the analysis already appear in the case that $n = p \cdot q$ where p, q are two distinct prime numbers. The notation in the more general case are very cumbersome, and we will therefore limit ourselves to this special case.

Let w be the nth root of unity, the DFT(n) is $Y_i = \sum_{j=0}^{n-1} w^{ij} y_j$ $(i = 0, 1,..., n-1)$, or more succinctly, $\mathbf{Y} = W_n \mathbf{y}$ *where* W_n is a matrix whose (i, j) entry is w^{ij} $(0 \leqslant i, j \leqslant n-1)$. It was pointed out in [9] and in [3] that if $n = a \cdot b$ where $(a, b) = 1$ then there exist permutation matrices Π_1, Π_2 such that $W_n = \Pi_1(W_a \times W_b)\Pi_2$, i.e., that up to permutations of rows and columns W_n is the tensor product of W_a and W_b. For the sake of completeness we will derive this result here.

Let k_1 $((k_1, a) = 1)$ and k_2 $((k_2, b) = 1)$ be two integers. If j_1 $(-(a-1) \leqslant j_1 \leqslant a-1)$ and j_2 $(-(b-1) \leqslant j_2 \leqslant b-1)$ are such that $k_1 \cdot bj_1 + k_2 aj_2 = 0 \bmod n$ $(n = ab)$ then $j_1 = j_2 = 0$. (Since $(k_1 \cdot b, a) = 1$ a divides j_1 and therefore $j_1 = 0$, and similarly for j_2). Therefore the mapping $t: \{0, 1,..., a-1\} \times \{0, 1,..., b-1\} \to \{0, 1,..., n-1\}$ defined by $t(j_1, j_2) = k_1 bj_1 + k_2 aj_2 \bmod n$ is one-one, and consequently onto.

Since $(a, b) = 1$ there exists integers r, s such that $ra + sb = 1$ (Note that $(s, a) = 1$ and $(r, b) = 1$). Define the mapping $t: \{0, 1, \ldots, a-1\} \times \{0, 1, \ldots, b-1\} \to \{0, 1, \ldots, n-1\}$ by $t(i_1, i_2) = sbi_1 + rai_2 \bmod n$, and the mapping $\tau: \{0, 1, \ldots, a-1\} \times \{0, 1, \ldots, b-1\} \to \{0, 1, \ldots, n-1\}$ by $\tau(j_1, j_2) = bj_1 + aj_2 \bmod n$. These two mappings were chosen because of the following property. Let $t(i_1, i_2) = k$ and $\tau(j_1, j_2) = l$ then $k \cdot l \bmod n = (sb_1 + rai_2)(bj_1 + aj_2) \bmod n = (sb)\, bi_1 j_1 + (ra)\, ai_2 j_2 \bmod n$. But $sb = 1 - ra$ and $ra = 1 - sb$ so we obtain $k \cdot l \bmod n = bi_1 j_1 + ai_2 j_2 \bmod n$.

Denote by $Y(i_1, i_2)$ that Y_k which satisfies $t(i_1, i_2) = k$, and by $y(j_1, j_2)$ that y_l which satisfies $\tau(j_1, j_2) = l$. Let $\mathbf{Y}(\ ,\ )$ denote the vectors of $Y(i_1, i_2)$'s arranged by lexicographical order, and $\mathbf{y}(\ ,\ )$ the vector whose coordinates are the $y(j_1, j_2)$'s arranged by lexicographical order. Since both t and τ are one-one there exist permutation matrices Π_1 and Π_2 such that $\mathbf{Y} = \Pi_1 \mathbf{Y}(\ ,\ )$ and $\mathbf{y} = \Pi_2 \mathbf{y}(\ ,\ )$. (Recall that $\mathbf{Y}$ and $\mathbf{y}$ are such that the DFT(n) is $\mathbf{Y} = W_n \mathbf{y}$).

Let $w_1 = w^b$ be the ath root of unity, and $w_2 = w^a$ be the bth root of unity. If $k = t(i_1, i_2)$ and $l = \tau(j_1, j_2)$ then $w^{k \cdot l} = w^{bi_1 j_1 + ai_2 j_2} = w_1^{i_1 j_1} \cdot w_2^{i_2 j_2}$. Therefore, $Y(i_1, i_2) = Y_k = \sum_{l=0}^{n-1} w^{k \cdot l} y_l = \sum_{j_1=0}^{a-1} \sum_{j_2=0}^{b-1} w_1^{i_1 j_1} \cdot w_2^{i_2 j_2} y(j_1, j_2)$. Consequantly the DFT($n$) can be written as $\mathbf{Y}(\ ,\ ) = (W_a \times W_b)\, \mathbf{y}(\ ,\ )$.

In order to analyze DFT($p \cdot q$) we have to study $w_p \times w_t$. To do that we will cast some of the discussion which appeared earlier in this section in somewhat different terms.

For each prime number p we define the $p \times p$ matrix A_p by

$$A_p = \begin{pmatrix} p^{-1} & -1 & -1 & & -1 \\ p^{-1} & 1 & 0 & & 0 \\ p^{-1} & 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots & & \vdots \\ p^{-1} & 0 & 0 & & 1 \end{pmatrix}.$$

The matrix A_p is non-singular, and in fact,

$$A_p^{-1} = \begin{pmatrix} 1 & 1 & 1 & \cdots & 1 \\ -p^{-1} & 1 - p^{-1} & -p^{-1} & \cdots & -p^{-1} \\ -p^{-1} & -p^{-1} & 1 - p^{-1} & \cdots & -p^{-1} \\ \vdots & & & & \\ -p^{-1} & -p^{-1} & p^{-1} & \cdots & 1 - p^{-1} \end{pmatrix}.$$

Direct calculations show that

$$W_p A_p = \left(\begin{array}{c|ccc} 1 & 0 & \cdots & 0 \\ \hline 0 & & & \\ \vdots & & \overline{W}_p & \\ 0 & & & \end{array}\right) = V_p,$$

where the (i,j)th entry of $\overline{W}_p$ is $w^{ij} - 1$ $(i,j = 1, 2, \ldots, p-1)$. The discussion (and notation) just prior to the statement of the Chinese Remainder Theorem shows that the coordinates of the vector $\overline{W}_p \cdot \mathbf{y}$ are the coefficients of the polynomial $T(u) = \sum_{i=0}^{p-2} (w(i) - 1)\, u^i)(\sum_{i=0}^{p-2} y(i)\, u^i) \bmod u^{p-1} - 1$. Since the minimal polynomial for w is $\sum_{i=0}^{p-1} u^i$, a linear combination (over Q) $\sum_{i=0}^{p-2} a_i w(i)$ is in Q if and only if all the a_i's are equal. Therefore $\{w(i) - 1\}$ are linearly independent and form a basis of $Q(w)$.

It was shown before that the $\mathrm{DFT}(p \cdot q)$ can be written as $(W_p \times W_q)\, \mathbf{y}(\ ,\ )$. Therefore, by renumbering the indices j of y_j, $\mathrm{DFT}(p \cdot q)$ can be written as $(W_p \times W_q) \cdot \mathbf{y}$. Since $W_p = V_p A_p^{-1}$, $W_q = V_q A_p^{-1}$, we obtain that $W_p \times W_q = (V_p \times V_q)(A_p^{-1} \times A_p^{-1})$. But $A_p^{-1} \times A_p^{-1}$ is invertible, then by Corollary 4 $\mu_B(\mathrm{DFT}(p \cdot q)) = \mu_B(V_p \times V_q)\, \mathbf{y})$ where $B = Q(w) \cup \{y_0, \ldots, y_{pq-1}\}$, w the (pq)th root of unity. By permuting rows and columns of $V_p \times V_q$ by a permutation matrix Π we obtain

$$\Pi^t (V_p \times V_q)\, \Pi = \left[\begin{array}{c|c|c|c} 1 & 0 & 0 & 0 \\ \hline 0 & \overline{W}_p & 0 & 0 \\ \hline 0 & 0 & \overline{W}_q & 0 \\ \hline 0 & 0 & 0 & \overline{W}_p \times \overline{W}_q \end{array}\right].$$

We have thus shown:

LEMMA 18. $\mu_B(\mathrm{DFT}(p \cdot q)) = \mu_B(\mathrm{DFT}(p), \mathrm{DFT}(q), (\overline{W}_p \times \overline{W}_q)\, y)$ *where* $B = Q(w) \cup \{y_0, y_1, \ldots, y_{pq-1}\}$, $G = Q$. *The remaining part of the analysis of* $\mu_B(\mathrm{DFT}(pq))$ *follows the approach used in* [10].

Let M be an $n \times m$ matrix such that coordinates of $M\mathbf{y}$ are the coefficients of $(\sum_{i=0}^{m-1} m_i u^i)(\sum_{i=0}^{m-1} y_i u^i) \bmod P(u)$, where P is a monic polynomial of degree m. Let N be an $n \times n$ matrix such that the coordinates of $N\mathbf{y}$ are the coefficients of $(\sum_{i=0}^{n-1} n_i v^i)(\sum_{i=0}^{n-1} y_i v^i) \bmod Q(v)$, where $Q(v)$ is a monic polynomial of degree n. Let $\mathbf{y}(\ ,\ )$ be a vector with the mn distinct indeterminates $y(i,j)$ $(0 \leqslant j \leqslant m-1$, $0 \leqslant j \leqslant n-1)$ as coordinates, which are arranged in lexicographical order. Let $\mathbf{y}(i_0, \ )$ be the vector whose coordinates are the $y(i_0, j)$'s. Using this terminology we can state:

LEMMA 19. *The coordinates of* $(M \times N)\, \mathbf{y}(\ ,\ )$ *are the coefficients of* $T(u, v) = (\sum_{j=0}^{n-1} \sum_{i=0}^{m-1} m_i n_j u_i v^j)(\sum_{j=0}^{n-1} \sum_{i=0}^{m-1} y(i,j)\, u^i v^j) \bmod (P(u), Q(v))$.

Proof. Let M_x be the $m \times m$ matrix such that the coefficients of $M_x\mathbf{y}$ are the coefficients of $T_x(u) = (\sum_{i=0}^{m-1} x_i u^i)(\sum_{i=0}^{m-1} y_i u^i) \bmod P(u)$, where the x_i's (as well as the y_j's) are distinct indeterminates. If G is a field which includes the coefficients of $P(u)$ then the entries of M_x are linear combinations of the x_i's

with coefficients in G. The (i,j) entry of M_x is the coefficient of y_j in t_i—the coefficient of u^i in $T_x(u)$. Let the (i,j) entry of M_x be $\sum_{i=0}^{m-1} g_i x_i$, then $M_{i,j} = \sum_{i=0}^{m-1} g_i m_i$. Similarly, the (i,j) entry of N is $\sum_{i=0}^{n-1} g_i n_i$ for some $g_i \in G$ (assuming G includes the coefficients of Q as well). Viewing $T(u,v) = (\sum_{i=0}^{m-1} m_i(\sum_{j=0}^{n-1} n_j v^j)u^i)$ $(\sum_{i=0}^{m-1}(\sum_{j=0}^{n-1} y(i,j)\, v^j)\, u^i) \bmod(P(u), Q(v))$ as a polynomial in u we see that $t_i(v)$—the coefficient of u^i in $T(u,v)$ can be written as $\sum_{k=0}^{m-1} r_{i,k}(v) \cdot (\sum_{j=0}^{n-1} y(k,j)v^j)$ $\bmod Q(v)$, where $r_{i,k}(v) = \sum_{k=0}^{m-1} g_k m_k(\sum_{j=0}^{n-1} n_j \cdot v^j) = (\sum_{k=0}^{m-1} g_k m_k)(\sum_{j=0}^{n-1} n_j v^j) = (M_{i,k})(\sum_{j=0}^{n-1} n_j v^j)$. By definition of N, the coefficient of v^j in $(\sum_{r=0}^{n-1} n_r v^r)$ $\sum_{r=0}^{n-1} y(k,r)\, v^j)$ is $\sum_{l=0}^{n-1} N_{jl} y(k,l)$. Therefore the coefficient of $y(k,l)$ in the coefficient of $u^i v^j$ of $T(u,v)$, which is the same as the coefficient of $y(k,l)$ in the coefficient of v^j in $t_i(v)$ is $M_{ik} \cdot N_{jl}$. This proves the lemma.

COROLLARY 13. *If we denote the coordinates of* $\mathbf{y}$ *by* $y(i,j)$ *arranged in lexicographical order then the coordinates of* $(\overline{W}_p \times \overline{W}_q)\,\mathbf{y}$ *are the coefficients of*

$$T(u,v) = \sum_{j=0}^{q-2} \sum_{i=0}^{p-2} (w_1(i) - 1)(w_2(j) - 1)\, u^i v^j \times \left(\sum_{j=0}^{q-1} \sum_{i=0}^{p-1} y(i,j)\, u^i v^j \right) \bmod(u^{p-1} - 1,\, u^{q-1} - 1).$$

where w_1 *is the* pth *root of unity,* w_2 *is the* qth *root of unity.*

Remark 21. Let w be the (pq)th root of unity. Since $[Q(w) : Q] = [Q(w_1 w_2) : Q] = (p-1)(q-1)$, we have that $[Q(w_1, w_2) : Q(w_1)] = q - 1$. Therefore $\sum_{i=0}^{q-1} u^i$ is irreducible (over $Q(w_1)$) and $\{w_2(j)\}$ is a basis of $Q(w)$ over $Q(w_1)$. Therefore $\{w_2(j) - 1\}$ form a basis of $Q(w)$ over $Q(w_1)$ and $\{(w_1(i) - 1)(w_2(j) - 1)\}$ form a basis of $Q(w)$ over Q and are consequently linearly independent (over Q).

Remark 22. Let $T(u,v)$ be as in Corollary 13. For every divisor d of $p - 1$, and d' of $q - 1$ define $T_{d,d'}(u,v) = T(u,v) \bmod(\Phi_d(u), \Phi_{d'}(v))$. (The Φ_r's are the cyclotomic polynomials.) Since $u^{p-1} - 1 = \prod_{d \mid p-1} \Phi_d(u)$, $v^{q-1} - 1 = \prod_{d' \mid q-1} \Phi_{d'}(v)$ we obtain by Remark 18 that $L_Q(C_{ff}(T)) = L_Q(\{C_{ff}(T_{d,d'}) \mid d$ divides $p - 1, d'$ divides $q - 1\})$. Let $R(u,v) = \sum_{j=0}^{q-1} \sum_{i=0}^{p-1} (w_1(i) - 1)(w_2(j) - 1) u^i v^j$ and let $R_{d,d'}(u,v) = R(u,v) \bmod(\Phi_d(u), \Phi_{d'}(v))$, then $L_Q(\{C_{ff}(R_{d,d'}) \mid d$ divides $p - 1$, d' divides $q - 1\}) = L_Q(\{(w_1(i) - 1)(w_2(j) - 1)\}) = Q(w)$. Since $\Phi_1(u) = u - 1, \Phi_1(v) = v - 1$, we have $R_{1,1} = \sum_{j=0}^{q-1} \sum_{i=0}^{p-1} (w_i(i) - 1)(w_2(j) - 1) = p \cdot f$, and therefore, $L_Q(\{\rho(C_{ff}(R_{d,d'})) \mid (d, d') \neq (1, 1)\}) = \rho(Q(w))$ (where ρ is the vector space homomorphism $\rho: Q(w) \to Q(w)/Q$. Let $S(u,v) = \sum_{j=0}^{q-1} \sum_{i=0}^{p-1} y(i,j)\, u^i v^j$. We define $S_{d,d'}(u,v) = S(u,v) \bmod(\Phi_d(u), \Phi_{d'}(v))$. Then $L_Q(C_{ff}(S)) = L_Q(\{C_{ff}(S_{d,d'})\})$.

For each d, d' we choose indeterminates $y'_{d,d'}(i,j)$ $(0 \leqslant i \leqslant \deg \Phi_d - 1$, $0 \leqslant j \leqslant \deg \Phi_{d'} - 1)$, $T_{d,d'}(u,v) = R_{d,d'}(u,v) \cdot (\sum_{i,j} y_{d,d'}(i,j)\, u^i v^j) \bmod(\Phi_d(u), \Phi_{d'}(v))$, where $R_{d,d'}$ is as in Remark 22.

LEMMA 20. *Let* $B = Q(w) \cup \{y_0, \ldots, y_{pq-1}\}$ $(w^{pq} = 1)$, $G = Q$, *then* $\mu_B(\mathrm{DFT}(pq)) = \mu_B(\mathrm{DFT}(p), \mathrm{DFT}(q), \{C_{ff}(T'_{d,d'}) \mid (d, d') \neq (1, 1)\})$.

Proof. By Lemma 18 and Corollary 13, $\mu_B(\mathrm{DFT}(pq)) = \mu_B(\mathrm{DFT}(p), \mathrm{DFT}(q), C_{ff}(T(u, v))$. By Remark 21, $\mu_B(\mathrm{DFT}(pq)) = \mu_B(\mathrm{DFT}(p), \mathrm{DFT}(q), \{C_{ff}(T_{d,d'}(u, v)) \mid (d, d') \neq (1, 1)\})$. By Remark 21, all the coefficients of all the coefficients of the $S_{d,d'}(u, v)$'s are linearly independent over Q, so there exists an invertible linear transformation (over Q) taking then to the set $\{y_{d,d'}(i,j)\}$. By Corollary 4, we obtain that $\mu_B(\mathrm{DFT}(p \cdot q)) = \mu_B(\mathrm{DFT}(p), \mathrm{DFT}(q), \{C_{ff}(T'_{d,d'}) \mid (d, d') \neq (1, 1)\})$.

To continue the analysis we have to study the multiplicative complexity of $C_{ff}(T_{d,d'})$.

LEMMA 21. *Let G and H be as in the statement of the Chinese Remainder Theorem, and let G be of characteristic 0. Let $P \in G[u]$ and $Q \in G[v]$ be irreducible monic polynomials. Let $P(a) = 0$ for a in some extension of G, and let $Q = \prod_{i=1}^{k} Q_i$ over $G(a)$. Let $Q_i(b_i) = 0$ for b_i in some extension of G, and let c_i be such that $G(a,b_i) = G(c_i)$. Let $P_i \in G[u]$ be a monic irreducible polynomial such that $P_i(c_i) = 0$ $(i = 1, 2, \ldots, k)$. Then there exists a homomorphism m: $H[u, v]/\langle P(u), Q(v) \rightarrow \bigtimes_{i=1}^{k} H[u]/\langle P_i(u)\rangle$, such that if we denote the components of m by $m_1, m_2, \ldots, m_l$ then for every polynomial $p(u, v) \in H[u, v]/\langle P(u), Q(v)\rangle$ $L_G(C_{ff}(p(u, v)) = L_G(\{C_{ff}(m_i(p))\ (i = 1, 2, \ldots, l\})$.*

Proof. Let H' be the ring of polynomials in $H[u]$ whose degree is smaller than $\deg(P(u))$, with addition and multiplication modulo $P(u)$. Then $H[u, v]/\langle P(u), Q(v)\rangle$ can be identified with $H'[v]/\langle Q(v)\rangle$. The ring H' includes the field G' of all polynomials whose coefficients are in G. G' is isomorphic to $G(a)$ (in fact, G' can be viewed as a particular representation of $G(a)$ taking $\{1, a_1, \ldots, a^{n-1}\}$ as a basis $(n = \deg(P))$. Replacing G in the Chinese Remainder Theorem by G', and viewing $Q(v)$ as being in $G'[u]$, we have $Q = \prod_{i=1}^{k} Q_i$, where the $Q_i \in G'[v]$ are monic irreducible polynomials. By the Chinese Remainder Theorem there exists a mapping m: $H'[v]/\langle Q\rangle \rightarrow \bigtimes_{i=1}^{k} [H'v]/\langle Q_i\rangle$ such that for every $p \in H'[v]/\langle Q\rangle$, $L_{G'}(C_{ff}(p)) = L_{G'}(\{C_{ff}(m_i(p))\})$. The elements of $H'[v]/\langle Q\rangle$ can be viewed as the algebra of a polynomial in $H[u, v]$ such that the degree of u is smaller than $\deg(P)$, and the degree of v is smaller than degree of Q_i, and where multiplication is defined by first multiplying modulo Q_i and then reducing modulo P. That is, $\{u^i v^j\}$ is a basis of this algebra, and $(u^i v^j) \cdot (u^k v^l) = (u^{i+k} \cdot (v^{j+l} \bmod Q_i) \bmod P)$. Since $\{1, a, \ldots, a^{n-1}\}$ is a basis of $G(a)$ (over G), and $\{1, b, b^2, \ldots, b^{m-1}\}$ is a basis of $G(a, b)$ over $G(a)$ (we denote the root of Q_i by b, and the degree of Q_i by m), then $\{a^i b^j\}$ is a basis of $G(a, b)$ over G. Moreover, if in $G(a, b)(a^i b^j \cdot (a^k b^l = \sum_{i,j} g_{i,j} a^i b^j$ for $g_{i,j} \in G$ then in $H'[v]/\langle Q_i\rangle (u^i v^j) \cdot (u^k v^l) = \sum_{i,j} g_{i,j} u^i v^j$.

Since $G(a, b)$ is a finite extension of G, there exists c such that $G(a, b) = G(c)$. Let P_i be the minimal polynomial for c (over G), and let r be the degree of P_i.

The set $\{1, c, c^2,..., c^{r-1}\}$ forms a basis of $G(a, b)$ and $a^i b^j = \sum_{k=0}^{r} h_k(i,j)\, c^k$, such that the matrix with entries in G whose kth column are the $h_k(i, j)$ is invertible. Let u' be an indeterminate and let α_i be the mapping $\alpha_i(u^i v^j) = \sum_{k=0}^{r} h_k(i,j)(u')^k$. We can lift α_i to a homomorphism α_i: $H'[v]/\langle Q_i\rangle \to H[u']/\langle P_i(u')\rangle$. For every polynomial $p(u, v) \in H'[v]/\langle Q_i\rangle$ $L_G(C_{ff}(p)) = L_G(C_{ff}(\alpha_i(p)))$ since the matrix defining the transformation is invertible. By the Chinese Remainder Theorem, for every element $p \in H[u, v]/\langle P, Q\rangle$ we have $L_G(C_{ff}(p)) = L_G(\{C_{ff}(m_i(p))\}) = L_G(\{C_{ff}(\alpha_i(m_i(p)))\})$. Finally, replace u' by u and we have proved the lemma.

Remark 23. By the definition of the P_i's it is clear that $\sum \deg P_i = (\deg P)(\deg Q)$.

For every two integers a and b we denote by $\Phi(a, b)$ the number of factors of the polynomial $\Phi_b(u)$ in the field $Q(w_a)$, where w_a is the ath root of unity. For every two numbers m, n we define $k(m, n) = \sum_{d'|n} \sum_{d|m} \Phi(d, d')$. Using this terminology we obtain:

THEOREM 5. $\mu_B(\mathrm{DFT}(p \cdot q)) \geqslant 2pq - p - q - k(p-1, q-1) - 3$, *where* $G = Q$, $B = Q(w) \cup \{y_0,..., y_{pq-1}\}$, $(w^{p \cdot q} = 1)$.

Proof. Let ν be the pth root of unity (p prime), and let W be the $p \times p$ matrix whose (i, j) entry is ν^{ij} $(0 \leqslant i, j \leqslant p-1)$. Let $\rho(W)$ be the $p \times p$ matrix whose (i, j) entry is $\rho(\nu^{ij})$. The rows of $\rho(W)$ are in $(Q(\nu)/Q)^p$. The first row of W is in Q^p, and the sum of all the rows of W is in Q^p, thus at most $p-2$ rows of $\rho(W)$ are linearly independent. But $\{\rho(\nu), \rho(\nu^2),..., \rho(\nu^{p-1})\}$ span $Q(\nu)/Q$, so exactly $p-2$ rows of $\rho(W)$ are linearly independent. By Remark 4, $\dim L_Q(r(\mathrm{DFT}(p))) = p-2$. The same argument shows that $\dim L_Q(r(\mathrm{DFT}(p)), r(\mathrm{DFT}(q))) = p + q - 4$. By Lemma 8 there exists a substitution α whose homogeneous part annihilates the indeterminates of DFT(p) and DFT(q) leaving the rest fixed. By Lemma 5 (and Lemma 19) $\mu_B(\mathrm{DFT}(pq)) = \mu_B(\mathrm{DFT}(p), \mathrm{DFT}(q), \{C_{ff}(T'_{d,d'} \mid (d, d') \neq (1, 1)\}) \geqslant \mu_B(\{C_{ff}(T'_{d,d'}) \mid (d, d') \neq (1, 1)\}) + p + q - 4$.

Let m be as in Lemma 20. We denote by $m(T'_{d,d'})$ the $\Phi(d, d')$ polynomials $\{m_i(T'_{d,d'})\}$. We will denote by $m(\Phi_d(u), \Phi_{d'}(v))$ the $\Phi(d, d')$ polynomial denoted by P_i in Lemma 20. By Remark 23, $\sum_i \deg P_i = (\deg \Phi_d)(\deg \Phi_{d'}) = \Phi(d)\,\Phi(d')$, (where $\Phi(n)$ is the Euler Φ function). Denote this set of $\{P_i\}$ by $s(d, d')$. Using Lemma 20 we obtain:

$$\mu_B(\{C_{ff}(T'_{d,d'}) \mid (d, d') \neq (1, 1)\}) = \mu_B(\{C_{ff}(m(T'_{d,d'})) \mid (d, d') \neq (1, 1)\}).$$

By the definition of $k(p-1, q-1)$ we obtain that the number of polynomials in $\bigcup_{(d,d')\neq(1,1)} S(d, d') = k(p-1, q-1) - 1$, and that

$$\sum_{(d,d')\neq(1,1)} \sum_{P \in S(d,d')} \deg(P) = \sum_{(d,d')\neq(1,1)} \Phi(d)\,\Phi(d')$$
$$= (p-1)(q-1) - 1 = pq - p - q.$$

Let R and $R_{d,d'}$ be as in Remark 22, then by Lemma 20 $L_Q(C_{ff}(R_{d,d'})) = L_Q(C_{ff}(m(R_{d,d'})))$, and by the Chinese Remainder Theorem we obtain (for w_1 the pth root of unity and w_2 the qth root of unity) that $L_Q(\{(w_1(i) - 1)(w_2(j) - 1)\}) = L_Q(C_{ff}(R)) = L_Q(\{C_{ff}(R_{d,d'})\}) = L_Q(\{C_{ff}(m(R_{d,d'}))\})$. By Remark 21 we obtain $L_Q(\{C_{ff}(m(R_{d,d'}))\}) = Q(w_1, w_2)$ and therefore $\dim L_Q(\{C_{ff}(m(R_{d,d'}))\}) = \dim Q(w_1, w_2) = (p-1)(q-1)$. But if we choose $d = d' = 1$ we have $R_{1,1} = \sum_{j=0}^{q-2}\sum_{i=0}^{p-2}(w_1(i) - 1)(w_2(j) - 1) = pq \in Q$, so $\dim L_Q(\rho\{C_{ff}(m(R'_{d,d'})) \mid (d, d') \neq (1, 1)\}) = \dim(Q(w_1, w_2))\, Q) = (p-1)(q-1) - 1 = pq - p - q$. By Corollary 10 we obtain $\mu_B(\{C_{ff}(m(T'_{d,d'})) \mid (d, d') \neq (1, 1)\}) = 2(pq - p - q) - (k(p-1, q-1) - 1) = 2pq - 2p - 2q + 1 - k(p-1, q-1)$, and therefore $\mu_B(\mathrm{DFT}(pq)) = 2pq - 2p - 2q + 1 - k(p-1, q-1) + p + q - 4 = 2pq - p - q - k(p-1, q-1) - 3$.

Remark 24. If we can prove the conjecture following Corollary 10, then we would have replace the $p + q - 4$ in the proof by $2p - \phi(p-1) - 3 + 2q - \phi(q-1) - 3$ (where $\phi(n)$ is as in Theorem 2), and then shown that $\mu_B(\mathrm{DFT}(pq)) = 2pq - (k(p-1, q-1) + \phi(p-1) + \phi(q-1) + 5)$.

In the rest of the section we will give a semi-closed-form of $\Phi(a, b)$ and $k(a, b)$.

LEMMA 22. *If $(a, b) = d$ then $\Phi(a, b) = \Phi(a) \cdot \Phi(b)/\Phi(c)$, where Φ is the Euler function, and $c = \text{l.c.}\, m(a, b) = ab/d$.*

Proof. Since $(a, b) = d$ there exist integers r and s such that $ra + sb = d$. Let w_1 be the ath root of unity, w_2 the bth root of unity, w_3 the cth root of unity and w_4 the (ab)th root of unity. Clearly, ${w_4}^d = w_3$, ${w_4}^a = w_3^{a/d} = w_2$, and ${w_4}^b = w_3^{b/d} = w_1$. These relations show that $w_1, w_2 \in Q(w_3$ and therefore $Q(w_1, w_2) \in Q(w_3)$. Since $w_3 = {w_4}^d = w_4^{ra} \cdot w_4^{sb} = ({w_4}^a)^r \cdot ({w_4}^b)^3 = {w_2}^r \cdot {w_1}^s \in Q(w_1, w_2)$ we have $Q(w_3 = Q(w_1, w_2))$. The minimal polynomial (over Q) of the nth root of unity t is of degree $\Phi(n)$ and has all the primitive nth root of unity as its roots, and for any w, v primitive nth roots of unity $Q(w) = Q(v)$. Let v be any primitive bth root of unity, then $Q(w_3) = Q(w_1, w_2) = Q(w_2)(w_1) = Q(v)(w_1 = Q(w_1, v) = Q(w_1)(v)$, and the degree of any primitive bth root of unity over $Q(w_1$ is $[Q(w_3) : Q(w_1)] = \Phi(c)/\Phi(a)$. Let P be any irreducible factor of the cyclotomic polynomial Φ_b over $Q(w_1$, then the roots of P are the primitive bth roots of unity, and therefore $\deg(P) = \Phi(c)/\Phi(a)$. So all the irreducible factors of Φ_b over $Q(w_1)$ have the same degree. Therefore $\Phi(b) = \sum \deg(P) = \Phi(a, b) \deg(P) = \Phi(a, b) \cdot \Phi(c)/\Phi(a)$, where the summation is over all the $\Phi(a, b)$ irreducible factors of Φ_b over $Q(w_1)$. This proves the lemma.

COROLLARY 14. *Let $a = a_1 \cdot a_2$, $b = b_1 \cdot b_2$ such that $(a_1, a_2) = (a_1, b_2) = (b_1, b_2) = (a_2, b_1) = 1$. Then $\Phi(a, b) = \Phi(a_1, b_1)\, \Phi(a_2, b_2)$.*

Proof. Let $c_1 = \text{l.c.m.}(a_1, b_1)$, $c_2 = \text{l.c.m.}(a_2, b_2)$, and $c = \text{l.c.m.}(a, b)$. By assumption we have $c = c_1 \cdot c_2$, $(c_1, c_2) = 1$. By properties of Euler Φ function

$\Phi(a) = \Phi(a_1)\,\Phi(a_2)$, $\Phi(b) = \Phi(b_1)\,\Phi(b_2)$, $\Phi(c) = \Phi(c_1)\,\Phi(c_2)$. So $\Phi(a, b) = \Phi(a)\,\Phi(b)/\Phi(c) = (\Phi(a_1)\,\Phi(b_1)/\Phi(c_1)) \cdot (\Phi(a_2)\,\Phi(b_2)(\Phi(c_2)) = \Phi(a_1, b_1)\,\Phi(a_2, b_2)$.

COROLLARY 15. *Let $a = p^r$, $b = p^s$, where p is a prime number, and let $t = \min(r, s)$, then*

$$\Phi(a, b) = \Phi(p^t) = \begin{cases} 1 & \text{if } t = 0 \\ (p-1)\,p^{t-1} & \text{if } t > 0 \end{cases}$$

THEOREM 6. $\Phi(a, b) = \Phi(gcd(a, b))$.

Proof. By Corollary 15, the statement holds if $a = p^r$, $b = p^s$. Let $a = p^r a_1$, $b = p^s b_1$, where $(p, a_1) = (p, b_1) = 1$. By Corollary 14, $\Phi(a, b) = \Phi(p^r, p^s)\,\Phi(a_1, b_1) = \Phi(gcd(p^r, p^s))\,\Phi(a_1, b_1)$. The theorem follows by induction on the number of prime divisors of l.c.m.(a, b).

We now turn our attention to $k(a, b)$.

LEMMA 22. *Let p be a prime number, then $k(p^r, p^r) = (p^{r+1} + p^r - 2)/(p-1)$.*

Proof. By induction on r. For $r = 0$, $k(1, 1) = 1$. Assume the lemma true for $r - 1$, then by definition

$$\begin{aligned} k(p^r, p^r) &= \sum_{j=0}^{r} \sum_{i=0}^{r} \Phi(p^i, p^j) \\ &= \Phi(p^r, p^r) + \sum_{j=0}^{r} \Phi(p^r, p^j) + \sum_{i=0}^{r} \Phi(p^i, p^r) + \sum_{j=0}^{r} \sum_{i=0}^{r} \Phi(p^i, p^j) \\ &= (p-1)\,p^{r-1} + p^{r-1} + p^{r-1} + k(p^{r-1}, p^{r-1}) \\ &= p^r + p^{r-1} + (p^r + p^{r-1} - 2)/(p-1) = (p^{r+1} + p^r - 2)/(p-1). \end{aligned}$$

LEMMA 23. *Let p be a prime and $s \geqslant r \geqslant 0$, then $k(p^s, p^r) = k(p^r, p^s) = ((s - r + 1)\,p^{r+1} - (s - r - 1)\,p^r - 2)/(p-1)$.*

Proof. It is clear that $k(p^s, p^r) = k(p^r, p^s)$ because $\Phi(\cdot, \cdot)$ is symmetric in its two variables.

$$\begin{aligned} k(p^s, p^r) &= \sum_{i=0}^{s-1} \sum_{j=0}^{r} \Phi(p^i, p^j) = \sum_{i=0}^{r} \sum_{j=0}^{r} \Phi(p^i, p^j) + \sum_{i=r+1}^{s} \sum_{j=0}^{r} \Phi(p^i, p^j) \\ &= k(p^r, p^r) + \sum_{i=r+1}^{s} \sum_{j=0}^{r} \Phi(p^j) = (p^{r+1} + p^r - 2)/(p-1) + (s-r)\,p^r \\ &= ((s - r + 1)\,p^{r+1} - (s - r - 1)\,p^r - 2)/(p-1). \end{aligned}$$

LEMMA 24. *Let* $a = a_1 \cdot a_2$ *and* $b = b_1 \cdot b_2$ *such that* $(a_1, a_2) = (a_1, b_2) = (b_1, b_2) = (b_1, a_2) = 1$, *then* $k(a, b) = k(a_1, b_1) \cdot k(a_2, b_2)$.

Proof. Every d which divides a can be written uniquely as $d = d_1 \cdot d_2$ where $d_1 \mid a_1$, $d_2 \mid a_2$. Similarly every d' which divides b can be written uniquely as $d_1' \cdot d_2'$. So

$$k(a, b) = \sum_{d' \mid b} \sum_{d \mid b} \phi(d, d') = \sum_{d_2' \mid b_2} \sum_{d_1' \mid b_1} \sum_{d_2 \mid a_2} \sum_{d_1 \mid a_1} \Phi(d_1 \cdot d_2, d_1' \cdot d_2').$$

By Corollary 14 we obtain

$$\begin{aligned} k(a, b) &= \sum_{d_1' \mid b_1} \sum_{d_1 \mid a_1} \sum_{d_2' \mid b_2} \sum_{d_2 \mid a_2} \Phi(d_1, d_1') \Phi(d_2, d_2') \\ &= \sum_{d_1' \mid b_1} \sum_{d_1 \mid a_1} \Phi(d_1, d_1') \sum_{d_2' \mid b_2} \sum_{d_2 \mid a_2} \Phi(d_2, d_2') \\ &= k(a_1, b_1)\, k(a_2, b_2). \end{aligned}$$

THEOREM 7. *Let* $a = \prod_{i=1}^{k} p_i^{\alpha_i}$, $b = \prod_{j=1}^{k} p_i^{\beta_i}$. *Let* $\gamma_i = \max(\alpha_i, \beta_i)$ *and* $\delta_i = \min(\alpha_i, \beta_i)$, *then*

$$k(a, b) = \prod_{i=1}^{k} ((\gamma_i - \delta_i + 1)\, p_i^{\delta_i + 1} - (\gamma_i - \delta_i -)\, p_i^{\delta_i} - 2)/(p_i - 1).$$

Proof. Theorem 7 is but repeated applications of Lemmas 23 and 24.

The proof of Theorem 5 can be used to obtain a lower bound of the DFT(n) for any n which has more than one prime divisor. The only difference is that the counterpart of the function k is much more complicated. Remark 24 can be extended to any square free number n, that is, if the Conjecture is true then the lower bound we will obtain using the Conjecture istead of the Theorem 1 is actually achievable.

ACKNOWLEDGMENT

The author wants to thank L. Auslander for his helpful suggestions about the writting of, as well as his careful reading of, the manuscript.

REFERENCES

1. S. WINOGRAD, Some bilinear forms whose multiplicative complexity depends on the field of constants, *Math. Systems Theory* **10** (1977), 169–180.
2. C. M. FIDUCCIA AND Y. ZALESTEIN, "Algebras Having Linear Multiplicative Complexities," Technical Report 46, Department of Computer Science, State University of New York, Stony Brook, N.Y., 1975.

3. S. WINOGARD, On computing the discrete fourier transform, *Math. Comp.* **32**, 141 141 (1978), 175–199.
4. J. W. COOLEY AND J. W. TUKEY, An algorithm for the machine calculations of complex Fourier series, *Math. Comp.* **19** (1965), 297–301.
5. S. WINOGRAD, On the number of multiplications necessary to compute certain functions, *Comm. Pure Appl. Math.* **23** (1970), 165–179.
6. C. M. FIDUCCIA, Fast matrix multiplication, *in* "Proceedings, Third Annual ACM Symposium on Theory of Computing, May 1971, pp. 45–49.
7. J. HOPCROFT AND L. KERR, Some techniques for proving certain simple programs optimal, *in* "IEEE Proceedings of Tenth Annual Symposium on Switching and Automata Theory, 1969, pp. 36–45.
8. C. M. RADER, Discrete Fourier Transform when the number of data samples is prime, *Proc. IEEE* **5**, 6 (1968), 1107–1108.
9. I. J. GOOD, The interaction of algorithm and practical Fourier series, *J. Roy. Statis. Soc. Ser. B.* 20 (1958), 361–372; addendum, **22** (1960), 372–375.
10. S. WINOGRAD, "On Multiplication of Polynomials Modulo a Polynomial," R. C. 6791, IBM Research, October 1977.